UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF INDIANA
INDIANAPOLIS DIVISION

STATE OF INDIANA EX REL. ROKITA, Plaintiff, v. APRIA HEALTHCARE LLC, Defendant.	CASE NO. _____ **COMPLAINT AND DEMAND** **FOR JURY TRIAL**

COMPLAINT FOR PERMANENT INJUNCTION, RESTITUTION, STATUTORY DAMAGES, CIVIL PENALTIES, AND OTHER EQUITABLE RELIEF

I. PRELIMINARY STATEMENT

The Plaintiff, Attorney General Todd Rokita, as *parens patriae* for the residents of the State of Indiana and on behalf of the State of Indiana in its sovereign capacity, by Deputy Attorneys General Hannah E. Jones, Joseph D. Yeoman, and Douglas S. Swetnam, files this Complaint for injunctive relief, restitution, statutory damages, civil penalties, attorneys' fees, the costs of this action, and other equitable relief against Apria Healthcare, LLC ("Apria") alleging violations of the Health Insurance Portability and Accountability Act of 1996, as amended by the Health Information Technology for Economic and Clinic Health Act of 2009, and Department of Health and Human Services Regulations, 45 C.F.R. § 160, *et seq*. (collectively referred to as "HIPAA"),

the Disclosure of Security Breach Act, Ind. Code § 24-4.9 ("DSBA"), and the Deceptive Consumer Sales Act, Ind. Code § 24-5-0.5-3 ("DCSA").

II. JURISDICTION AND VENUE

1. The Court has jurisdiction for this cause of action pursuant to 42 U.S.C. § 1320d-5(d) and 28 U.S.C. § 1331.

2. Venue in this District is proper pursuant to 28 U.S.C. § 1391(b)(2), (c) and (d).

3. Plaintiff, the Attorney General of the State of Indiana, has provided notice of this action to the Secretary of Health and Human Services as required under 42 U.S.C. § 1320d-5(d)(4).

III. PARTIES

4. Plaintiff, the Attorney General of the State of Indiana, is authorized to bring this action and to seek injunctive and other statutory relief pursuant to 42 U.S.C. § 1320d-5(d)(1).

5. During all times relevant to this Complaint, Apria was a Delaware limited liability company.

6. Apria is headquartered in Indianapolis, Indiana at 7353 Company Dr, Indianapolis, IN 46237.

7. During all times relevant to this Complaint, Apria was engaged in business in the Southern District of Indiana, operating as a health equipment provider that sold products and services to Indiana residents and other Americans.

8. According to Apria's marketing, it "is a leading provider of home healthcare equipment and related services across the USA, serving approximately 2 million patients from our 270+ locations."[1]

[1] *About Us*, APRIA, https://www.apria.com/about-us (last visited Feb. 23, 2024).

9. Apria provides multiple at-home health care products and services including treatment for sleep apnea, respiratory issues, diabetes, wounds, as well as a general pharmacy.

10. The services provided by Apria are geared towards caring for an older population.[2]

11. Further, Apria's marketing on its website makes it clear that Apria is marketing to an older population.

12. Apria is wholly owned by Owens & Minor, Inc. ("Owens & Minor").

13. Owens & Minor is a corporation headquartered in Virginia.

14. Owens & Minor markets itself as "Global healthcare solutions that provide essential products and services to support care from the hospital to the home."[3]

IV. HIPAA AND HITECH BACKGROUND

15. On August 21, 1996, HIPAA was passed, and with it, provisions that required Health and Human Services ("HHS") to adopt national standards for the security and privacy of electronic health care transactions.

16. In December of 2000, HHS promulgated the Privacy Rule. It was later modified in August of 2002. Compliance with the Privacy Rule was required as of April 14, 2003.

17. In the August 2002 notice of the final rule, HHS wrote:

> The use of these standards will improve the efficiency and effectiveness of public and private health programs and health care services by providing enhanced protections for individually identifiable health information. These protections will begin to address growing public concerns that advances in electronic

[2] There are many factors that can cause sleep apnea. One of those factors is age. The risk of sleep apnea increases between the ages of 30 and 70. *Sleep Apnea Statistics and Facts You Should Know*, NATIONAL COUNCIL ON AGING (Oct. 4, 2023), https://www.ncoa.org/adviser/sleep/sleep-apnea-statistics/#:~:text=The%20risk%20increases%20between%20ages,a%20higher%20prevalence%20of%20OSA. The onset of type 2 diabetes is the most common in people who are 45-64 years old. *The average age of onset for type 2 diabetes*, MEDICALNEWSTODAY (Apr. 28, 2023), https://www.medicalnewstoday.com/articles/317375#:~:text=The%20average%20age%20of%20onset%20for%20type%202%20diabetes&text=The%20onset%20of%20type%202,diabetes%20in%20the%20United%20States.

[3] *OM Like Takes Care*, OWENS & MINOR, https://www.owens-minor.com/ (last visited Feb. 23, 2024).

> technology and evolution in the health care industry are resulting, or may result, in a substantial erosion of the privacy surrounding individually identifiable health information maintained by health care providers, health plans and their administrative contractors. . . .
>
> This regulation has three major purposes: (1) To protect and enhance the rights of consumers by providing them access to their health information and controlling the inappropriate use of that information; (2) to improve the quality of health care in the U.S. by restoring trust in the health care system among consumers, health care professionals, and the multitude of organizations and individuals committed to the delivery of care; and (3) to improve the efficiency and effectiveness of health care delivery by creating a national framework for health privacy protection that builds on efforts by states, health systems, and individual organizations and individuals.

Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg, 82462-01 (Dec. 28, 2000) (to be codified at 45 C.F.R. parts 160 and 164), https://www.govinfo.gov/content/pkg/FR-2000-12-28/pdf/00-32678.pdf.

18. In February of 2003, HHS promulgated the Security Rule. Compliance with the Security Rule was required as of April 20, 2005.

19. In the February 2003 notice of the final rule, HHS wrote:

> [H]ealth care providers . . . must assure their customers (for example, patients, insured individuals, providers, and health plans) that the integrity, confidentiality, and availability of electronic protected health information they collect, maintain, use, or transmit is protected. The confidentiality of health information is threatened not only by the risk of improper access to stored information, but also by the risk of interception during electronic transmission of the information. The purpose of this final rule is to adopt national standards for safeguards to protect the confidentiality, integrity, and availability of electronic protected health information.

Health Insurance Reform: Security Standards, 68 FR 8334-01 (Feb. 20, 2003) (to be codified as 45 C.F.R. parts 160, 162, and 164), https://www.govinfo.gov/content/pkg/FR-2003-02-20/pdf/03-3877.pdf.

20. As part of the American Recovery Act of 2009, the Health Information Technology for Clinical and Economic Health ("HITECH") Act was passed. It gave State Attorneys General the authority to enforce HIPAA and its regulations.

21. On January 25, 2013, HHS promulgated a final Omnibus rule which implemented provisions in the HITECH Act, including adding the Breach Notification Rule. Compliance with the Breach Notification Rule and other provisions was required as of September 23, 2013.

22. The statute of limitations for violation of HIPAA is six years. 42 U.S.C. § 1320a–7a(c)(1) and 42 U.S.C. § 1320d-5(d)(7).

V. FACTUAL ALLEGATIONS

The Data Breaches

23. On or around April 5, 2019, an unauthorized third-party or parties ("the Intruder") gained access to Apria's environment. On or around August 27, 2021, more than two years after the first breach, the Intruder gained access to Apria's environment for a second time. Together, these two data breaches will be referred to as the "Data Breaches." According to the CrowdStrike report, Apria's system was penetrated multiple times by the same intruder or intruders.[4]

24. On or around April 5, 2019, the Intruder did this by using the privileged email account of Apria's Infrastructure Technical Lead.

[4] At the time of this filing, Plaintiff has no way to ascertain if this information is true. For clarity, "the Intruder" is meant to signify both a single intruder, as described in the CrowdStrike report, and the possibility of multiple intruders.

25. The Intruder was able to use this email account 49 times to log in to Apria's system between April 5, 2019 and May 3, 2019.

26. Later, forensic investigators were unable to determine the cause of the compromise of the credentials; however, it appears that a phishing email was sent to the Infrastructure Technical Lead.

27. Apria decided not to investigate further due to the cost.

28. On or around April 27, 2019, the Intruder used the Infrastructure Technical Lead's email account to create a new account: exchhealth@apriahc.onmicrosoft.com.

29. This new account was then granted "FullAccess" permissions to six (6) mailboxes. This allowed the Intruder to open these persons' email boxes, read the contents, and manage the contents.

30. The Intruder used the new account to access six (6) user mailboxes in the Apria environment a total of 93 times.

31. The six (6) user mailboxes included mailboxes for:

a. Chief Human Recourses Officer;

b. Director, Application;

c. VP of eCommerce; formerly Manager, Customer Service;

d. Team Manager, eCommerce;

e. VP, eCommerce; and

f. Company Newsletter Publisher; Intranet Content Manager; Corporate Events Manager.

32. Based on the documents provided by Apria, the Intruder went through these persons' email inboxes and emails. At the time of filing, it is unclear if and what was exfiltrated out of Apria's system with regards to the 2019 breach.

33. Upon information and belief, Apria did not notify Indiana consumers of the 2019 breach until 2023.

34. On or around August 27, 2021, more than two years after the first breach, the Intruder leveraged exchhealth@apriahc.onmicrosoft.com to gain access to the Apria environment.

35. Upon information and belief, Apria did not discover and/or delete exchhealth@apriahc.onmicrosoft.com at any point in time between April 27, 2019 to August 27, 2021.

36. Upon information and belief, Apria did not discover that any of the compromised emails above at any point in time between April 27, 2019 to August 27, 2021.

37. On or around August 27, 2021, the Intruder reset exchhealth@apriahc.onmicrosoft.com password and used the account to gain access to Apria's Citrix environment.

38. The Intruder used another Apria employee's email account to grant exchhealth@apriahc.onmicrosoft.com access to more email boxes.

39. This employee was a System Administrator.

40. From August 27, 2021 through September 1, 2021, the Intruder used the System Administrator's account to grant the exchhealth@apriahc.onmicrosoft.com access to 14 mailboxes,

41. The 14 mailboxes included the mailboxes for:

a. Dan Starck, CEO of Apria;

b. Chief Human Resources Officer;

c. VP of eCommerce; formerly Manager of Customer Service;

d. Director of Applications;

e. Senior Network Engineer;

f. Senior Systems Analyst;

g. Team Manager of eCommerce;

h. Manager of Application;

i. Lead Accounts Payable Clerk;

j. Systems Administrator;

k. eCommerce Operations Specialist;

l. Administrative Assistant to the CEO, CFO, and Chief HR Officer;

m. Administrative Assistant; and

n. the Apria Newsletter, which was the account managing the Magento system used by the e-Commerce platform for Apria Direct.

42. The Intruder leveraged three (3) administrative accounts to laterally move through ten (10) of Apria's systems.

43. Using exchhealth@apriahc.onmicrosoft.com, the Intruder logged in 119 times.

44. The Intruder was able to access the 14 mailboxes a total of 268 times.

45. Upon information and belief, there was nothing in Apria's system that blocked the Intruder's access to these systems and/or accounts.

46. On or around September 1, 2021, the Intruder reset the password to the administrator account associated with Apria's e-commerce website.

47. On or around September 1, 2021, the Federal Bureau of Investigation ("FBI") contacted Apria by telephone to inform Apria that the Intruder the FBI was tracking may have gained access to Apria's email environment.

48. Apria contacted CrowdStrike to begin a forensic examination and to disable known compromised accounts and block network access to IP addresses associated with the Intruder to "restrict the [Intruder's] access to the environment."

49. From September 1, 2021 to October 10, 2021, the Intruder installed ScreenConnect2, which allowed the Intruder to maintain access to the Apria environment.

50. The last outbound communication to the Intruder's ScreenConnect2 Server occurred on October 10, 2021.

51. The Intruder accessed at least 424 files and 25 systems across Apria's environment.

52. At the time of the attack, Apria did not have two-factor or multi-factor authentication in place.

Consumer Information Was Compromised and Disclosed

53. As a result of the Data Breaches, Indiana residents' information was compromised by the Intruder.

54. As a result of the Data Breaches, Indiana residents' information was disclosed to the Intruder.

55. At least 1,869,598 people were impacted by the Data Breaches.

56. Of the people impacted, at least 42,021 were Indiana residents.

57. This customer information, including for Hoosiers, included:

a. Alien Registration Number;

b. Birth Certificate;

c. Certificate/license number;

d. Credit/Debit Card Number with Password or Security Code;

e. Credit/Debit Card Number without Password or Security Code;

f. Date of Birth;

g. Device Descriptions;

h. Driver's License Number;

i. Health Benefits and Enrollment Information;

j. Health Insurance Application or Claims Information;

k. Health Insurance Policy or Subscriber Number;

l. Individual Taxpayer Identification Number;

m. IRS e-file PIN;

n. Marriage Certificate;

o. Medical Device identifiers and serial numbers;

p. Medical History;

q. Passport Number;

r. Patient Account Number;

s. Patient Address;

t. Patient Date of Death;

u. Patient Dates of Service;

v. Patient Email Address;

w. Patient Fax number;

x. Patient Internet Protocol Address;

y. Patient License plate Number;

z. Patient Medical Record Number;

aa. Patient Name;

bb. Patient Telephone Number;

cc. Patient Web URL;

dd. Prescription Information;

ee. Security Code or Password to a Financial Account;

ff. Security Code, Access Code, or Password to a non-financial account;

gg. Social Security Number;

hh. Username and Password;

ii. Workers Compensation Claim or Health Information.

58. Some of the information compromised was Protected Health Information ("PHI") and/or Electronic Protected Health Information ("ePHI").

59. Some of the information disclosed was PHI and/or ePHI.

60. Some of the information compromised was Personal Information, as defined by Ind. Code § 24-4.9-2-10.

61. Some of the information disclosed was Personal Information, as defined by Ind. Code § 24-4.9-2-10.

62. All of the information compromised and/or disclosed was highly sensitive information that could result in identity deception, as defined by Ind. Code § 35-43-5-3.5, identity theft, or fraud of Hoosiers.

63. Apria had a responsibility to implement and maintain reasonable procedures to protect and safeguard this information from unlawful use or disclosure.

64. Apria did not implement and maintain reasonable procedures to protect and safeguard this information from unlawful use or disclosure.

65. As of this filing, Apria has not implemented reasonable procedures to protect and safeguard this information from unlawful use or disclosure.

66. From April 5, 2019 until October 10, 2021, Apria's system or systems to store and/or collect PI and PHI was compromised by an unauthorized third-party or parties.

67. Apria did not have reasonable monitoring policies, procedures, and/or mechanisms in place.

68. If Apria had taken reasonable steps to monitor its systems, Apria would have mitigated the Data Breaches.

69. Apria did not have reasonable access control policies, procedures, and/or mechanisms in place.

70. If Apria had taken reasonable steps to control who had access to its systems, Apria would have mitigated the Data Breaches.

71. For years, reputable third parties warned Apria of deficiencies in Apria's systems and Apria's policies and procedures.

72. If Apria had acted on these warnings, Apria would have mitigated the Data Breaches.

73. Apria had many opportunities to take reasonable steps to protect this sensitive data.

74. Apria had many opportunities to mitigate the harm done to Hoosiers by these Data Breaches.

75. Instead, Apria chose not to take reasonable steps to protect this sensitive data, which put Hoosiers at risk.

Breach Notification Timeline

76. Apria's notification to Indiana consumers, the Office of the Indiana Attorney General, and the credit reporting agencies was extremely delayed.

77. Apria's delay in notifying Indiana consumers, the Office of the Indiana Attorney General, and the credit reporting agencies was unreasonable.

78. By having an extreme delay in notifying Indiana consumers, the Office of the Indiana Attorney General, and the credit reporting agencies, Apria greatly increased the chance that Hoosiers were the victims of identity deception, as defined by Ind. Code § 35-43-5-3.5, identity theft, or fraud.

79. Apria had many opportunities to alert Hoosiers of the Data Breaches, but Apria chose not to.

80. Instead, Apria chose to delay notification for close to two years, which put Hoosiers' identities at risk.

81. From approximately April 5, 2019 to May 4, 2019, the Intruder gained unauthorized access to Apria's systems.

82. From approximately April 5, 2019 to May 4, 2019, the Intruder had continuous access to Apria's system.

83. On June 28, 2021, members of Apria's senior management team met with members of Owens & Minor's senior management team to discuss a potential transaction between the two companies.

84. According to the CrowdStrike report, there was no activity by the Intruder from May 7, 2019 to August 27, 2021.

85. According to the CrowdStrike report, on August 27, 2021, the Intruder then began accessing Apria's system again.

86. On or around September 1, 2021, the Federal Bureau of Investigation ("FBI") contacted Apria. The FBI informed Apria that the FBI was tracking a threat actor, and that the FBI believed the Intruder may have gained access to Apria's systems.

87. If not for the FBI notifying Apria, it is unlikely that Apria would have ever discovered the breach.

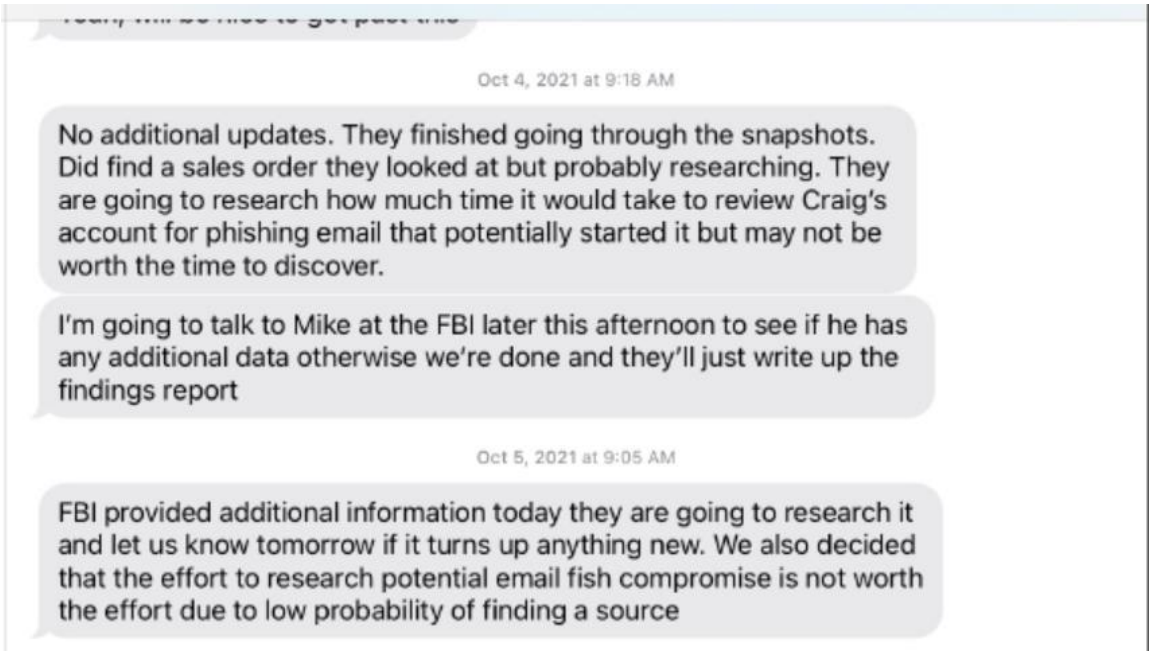
88. On or around September 1, 2021, Apria hired CrowdStrike[5] to conduct a forensic investigation of the Data Breaches.

89. On October 4, 2021, Jerry Walters, Apria's Security Official sent a text message from his personal phone, using a personal email address, stating CrowdStrike was looking into the Infrastructure Technical Lead's email account to find the "phishing email that potentially started [the Breaches]" but it might not be worth Apria's time to look into this further.

90. On October 5, 2021, Jerry Walters sent another text message stating Apria decided not to investigate the phishing email.

91. Below is an example of Jerry Walters' texts on October 4 and 5, 2021:

[5] CrowdStrike is an Austin, TX based cybersecurity and technology company. CrowdStrike offers cyberattack response and forensic investigations as services. *See Services*, CROWDSTRIKE, https://www.crowdstrike.com/services/ (last visited Feb. 28, 2024).



92. CrowdStrike completed its forensic analysis on or around October 27, 2021 and sent over its report to Apria on November 5, 2021.

93. On or around November 22, 2021, CrowdStrike informed Apria that the Intruder had the capability to access more emails than originally listed.

94. On December 7, 2021—approximately 98 days after Apria was informed of the Data Breaches by the FBI—, Apria began to request quotes from third-party e-discovery vendors.

95. On January 10, 2022, Owens & Minor announced in a press release that Owens & Minor signed a definitive agreement to acquire Apria.

96. Apria provided a list of its previous data incidents, including the Data Breaches from this Complaint, to Owens and Minor during contract negotiations. At this time, Plaintiff does not know the date in which Apria disclosed the Data Breaches to Owens & Minor.

97. The disclosure provided to Owens & Minor states: "Citrix Breach – Cyber criminals accessed the internal [Apria] network and Office365 environment as if they were [Apria] employees with high-level permissions. The criminals had access between April 2019 and May

2019, and between August 27, 2021 and October 10, 2021. Apria is working with outside counsel to complete analysis on any notification/reporting obligations."

98. On January 20, 2022, Apria received quotes from multiple third-party e-discovery firms.

99. On March 29, 2022, the transaction between Owens & Minor and Apria closed, and Apria was acquired by Owens & Minor.

100. On April 1, 2022, Apria replaced their former general counsel with new general counsel.

101. On April 13, 2022, Apria's new general counsel met with outside counsel to discuss the Data Breaches and next steps.

102. On May 4, 2022, Apria's counsel requested a master service agreement ("MSA") and statement of work ("SOW") from a third-party e-discovery firm, Palo Alto ("Discovery Vendor"), to conduct an initial review of potentially accessed data.

103. On May 16, 2022, before securing a discovery vendor, Apria notified Health and Human Services ("HHS") of the breach.

104. Apria's notification to HHS claimed only one person's PHI was identified in the initial investigation.

105. In Apria's notice to HHS, Apria claimed at the time of reporting, the investigation into the breach was not complete and promised to provide an additional update. Apria did not provide any updates until May 22, 2023.

106. On May 26, 2022, Apria's counsel executed a Business Associate Agreement ("BAA") between Apria and the Discovery Vendor – 170 days after Apria started their search for an e-discovery firm and 258 days since the discovery of the Data Breaches.

107. On June 7, 2022—12 days after a BAA was executed—, Apria met with its insurance company to discuss the Discovery Vendor's contract.

108. On June 9, 2022, Apria's counsel provided the insurer with all prior e-discovery vendor quotes, the executed MSA, executed BAA, and the proposed SOW for the Discovery Vendor.

109. On June 15, 2022, Apria and the Discovery Vendor finalized the contract.

a. 226 days after notice was required to be sent under HIPAA;

b. 288 days after the discovery of the Data Breaches; and

c. 1,167 days after first breach occurred.

110. A secure portal for data transmission was made available on June 15, 2022. Apria did not complete uploading the data until June 25, 2022.

111. On or around July 8, 2022, the Discovery Vendor provided Apria with its initial assessment of all individuals affected by the breach.

112. On or around July 13, 2022, Apria's counsel met with the Discovery Vendor, to discuss changing search terms and excluding human resource policies and procedures.

113. On or around July 17, 2022, the Discovery Vendor provided Apria an updated search results report.

114. On or around July 22, 2022, Apria started a contract dispute with the Discovery Vendor.

115. On or around August 17, 2022, Apria executed a SOW with the Discovery Vendor.

116. On or around August 18, 2022, Apria requested the Discovery Vendor manually review the documents and files that were potentially accessed and contained PHI.

117. On or around September 23, 2022, the Discovery Vendor claimed that 96% of files had been reviewed with fewer than 10% containing potential Personal Information ("PI") and/or PHI, but some larger files would need an extra five (5) to eight (8) days to review.

118. On or around September 28, 2022, Apria's counsel and the Discovery Vendor had a phone call to clarify what the Discovery Vendor should be looking for within the documents. At the time, the Discovery Vendor did not provide final results.

119. On or around October 12, 2022, the Discovery Vendor informed Apria's counsel that it was still reviewing data.

120. Further, the Discovery Vendor identified 17 million records that possibly contained PHI and estimated there would be an additional 3-5 million records once the review was completed.

121. On or around October 18, 2022, Apria's counsel met with the Discovery Vendor to consolidate records and remove duplicates. After consolidation, the Discovery Vendor identified 12 million records.[6]

122. On or around February 6, 2023, after months of back and forth, a final list of personal data of potentially affected individuals was provided to Apria.

123. Apria and Apria's counsel did not start reviewing the data provided by the Discovery Vendor until March 24, 2023.

a. 46 days after Apria received the results;

b. 508 days after notice was required to be sent under HIPAA;

c. 570 days after the discovery of the Data Breaches; and

[6] From the documents provided by the Defendant, Plaintiff currently does not know what Apria's Discovery Vendor meant by "record."

d. 1,449 days after first breach occurred.

124. On or around March 28, 2023, Apria's counsel requested quotes from a notification vendor to provide address verification, mailing, and to create a call center.

125. On or around April 21, 2023, Apria's insurer approved of the notification vendor's proposal and Apria's counsel began negotiating the contract.

126. On or around May 2, 2023, Apria reviewed the data file provided by the Discovery Vendor to assess whether each person was a patient or employee and whether Apria had a known address.

127. On or around May 4, 2023, Apria's counsel engaged an address vendor to help identify missing or partially missing addresses.

128. On or around May 5, 2023, Apria's counsel signed a contract with the notification vender.

129. On or around May 5, 2023, Apria received review files[7] from the Discovery Vendor related to known employees.

130. On or around May 10, 2023, Apria's counsel engaged a public relations vendor to assist in drafting a press release and other communications regarding the breach.

131. On or around May 12, 2023, the address vendor provided an additional 34,768 addresses to Apria.

132. On or around May 22, 2023, Apria provided notification to the Indiana Attorney General's office.

[7] From the documents provided by the Defendant, Plaintiff currently does not know what Apria's Discovery Vendor meant by "review files."

133. On or around May 22, 2023, Apria sent out a national press release about the Data Breaches.[8]

134. On or around May 22, 2023, Apria added a warning on their website.[9]

135. The last known time the breach notice was on Apria's website is January 20, 2024. The notice is no longer on the website. Apria left the notice up for approximately 122 days, but it took Apria 629 days to let their customers know that there was a data breach.

136. On or around May 22, 2023, Apria provided the data file of all potentially affected individuals to the notification vender.

137. On or around May 25, 2023, the notification vendor began looking through the National Change of Address data base ("NCOA").

138. On or around May 31, 2023, Apria's counsel approved NCOA results and final notification letter proofs.

139. On or around June 1, 2023, the notification vendor performed quality control checks with the print vendor.

140. On or around June 6, 2023, the print vendor printed and mailed the first 75,000 letters.

a. 120 days after Apria received the final list of personal data of potentially affected individuals;

b. 582 days after notice was required to be sent under HIPAA;

c. 644 days after the discovery of the Data Breaches; and

[8] *Apria Notice of Data Breach*, BUSINESS WIRE, https://www.businesswire.com/news/home/20230522005644/en/Apria-Notice-of-Data-Breach (last visited Feb. 28, 2024).
[9] Apria Homepage, WAYBACK MACHINE INTERNET ARCHIVE (Jan. 20, 2024), https://web.archive.org/web/20240120045207/[http://www.apria.com/].

d. 1,523 days after first breach occurred.

141. The first group of individuals did not receive notice of the Data Breaches until 644 days after the breach.

142. Between June 7, 2023 and August 7, 2023, the print vendor mailed approximately 300,000 letters every weekday until all individuals with valid addresses received notice.

a. 182 days after Apria received the final list of personal data of potentially affected individuals;

b. 644 days after notice was required to be sent under HIPAA;

c. 705 days after the discovery of the Data Breaches; and

d. 1,585 days after first breach occurred.

Apria's Website

143. Apria's website has been live since at least February 10, 1999.

144. At all times relevant to this Complaint and at the time of this filing, Apria's websites allowed consumers, including Hoosiers, the ability to:

a. Log in to an account;

b. Pay a bill;

c. Shop on an e-commerce platform;

d. Submit orders;

e. Transfer services to Apria;

f. Contact Apria; and more.

145. At a minimum, Apria's websites allowed consumers, including Hoosiers, to provide Apria with a payment card (including debit and credit cards), other payment information,

PHI, and other personal information, which includes social security numbers and driver's license information.

146. Further, it allowed consumers, including Hoosiers, the ability to sign up for Apria's newsletter which was circulated by a compromised email account.

147. On the website, Apria includes multiple statements ensuring the protection of patient privacy.

148. Statements include: "[Apria] maintain[s] commercially reasonable security measures to protect the personal data we collect and store from loss, misuse, destruction, or unauthorized access." [10]

149. And: "Apria… respects the privacy of your information."[11]

150. Between September 1, 2021 and October 10, 2021 – a time that Apria knew the Intruder was in their system – Apria's website was still actively accepting payments and allowing patients to submit PI and PHI to Apria.

151. This was despite Apria having actual knowledge their systems were not secure.

Apria's HIPAA Policies

152. During all times relevant to this Complaint, Apria was a Covered Entity under 45 C.F.R. §160.103, and from time to time, functioned as a Business Associate.

153. During all times relevant to this Complaint, Apria engaged in the electronic exchange in health care data for the purposes of, including, but not limited to, coordinating insurance benefits for their patients and payment and remittance of services rendered.

154. On June 29, 2023, Plaintiff issued a Civil Investigative Demand ("CID") to Apria.

[10] Apria Privacy Policy, APRIA, https://www.apria.com/privacy-policy (last visited Feb. 28, 2024).
[11] *Id.*

155. In response to the CID, Apria provided a copy of their HIPAA policies and other business-wide policies.

156. Apria's HIPAA policies did not ensure appropriate PHI access.

157. Apria did not have information access management policies.

158. Apria's policies did not separate PHI from other operations.

159. Apria's policies did not implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network.

160. Apria's policies did not implement electronic mechanisms to corroborate that electronic protected health information has not been altered or destroyed in an unauthorized manner.

161. Apria's "Security Management Policy" stated Apria's security policies should be reviewed and evaluated annually.

162. In practice, Apria's 2021 Risk Assessment indicates that Apria did not review and update on an annual basis.

163. Apria's "Security Management Policy" stated that employees and non-employees should participate in ongoing information security awareness training and briefings.

164. In practice, Apria's 2021 Risk Assessment indicated that non-employees are not receiving training.

165. Further, not all Apria employees were completing the training that was sent to them.

166. Apria's "Risk Management Policy" stated that Apria categorizes each information system to determine the sensitivity of the information being processed, stored, and transmitted by the system.

167. In practice, Apria's 2021 Risk Assessment stated that there was no data classification policy.

168. Apria's "Risk Management Policy" stated that if a risk assessment indicated that existing security controls are not sufficient, the Information Technology Security & Compliance group would evaluate and implement additional security controls.

169. Apria received four risk assessments indicating that security controls were not sufficient.

170. According to Apria's Security Narratives, Apria made limited changes year-to-year to their security controls.

171. Apria's "Risk Management Policy" states that if any issues identified during a risk assessment, they will be addressed appropriately.

172. In practice, Apria's Risk Assessments for 2018, 2020, and 2021 indicated that Apria did not fix vulnerabilities in a timely manner.

173. Apria's "Risk Management Policy" required risk assessments to be performed on a "regular basis."

174. Apria conducted risk assessments on May 5, 2018, July 14, 2020, October 20, 2020, October 25, 2021, and December 14, 2022.

175. Apria did not conduct a risk assessment in 2019 – the year of the first Data Breach.

176. Apria's "Access Control Policy" stated that all users of Apria's technology systems must be identified and authenticated before accessing information.

177. In practice, Apria's 2020 Risk Assessment indicated that all employees were able to access ePHI without using a login.

178. Apria's "Access Control Policy" required periodic reviews of employees and non-employees accounts to ensure that the "appropriate minimum privileges are granted and unauthorized accounts have been removed."

179. Upon information and belief, Apria had not reviewed employee and non-employee access.

180. If Apria had reviewed employee and non-employee access, Apria would have discovered the Data Breaches.

181. Apria only discovered the Data Breaches after a third-party notified it.

182. Apria's "Access Control Policy" required a unique user ID and password to access Apria's information technology systems.

183. In practice, Apria's 2020 Risk Assessment stated ePHI was accessible to all employees without a login.

184. Apria did not require employees to change their passwords unless it is "known or suspected to be compromised or easily guessable."

185. Apria's "Operations Management Policy" was designed to limit access to protected information in non-production environments.

186. In practice, the Risk Assessments for 2018, 2020, and 2021 indicated that ePHI was pervasive in Apria's systems; that there was no record or map of where ePHI is located; and there was no data classification policy.

187. Apria's "Security Monitoring and Response Policy" stated that Apria should implement logging and monitoring "where reasonable".

188. Upon information and belief, Apria had not implemented logging and monitoring.

189. If Apria had been logging and monitoring, Apria would have discovered the Data Breaches. Apria only discovered the Data Breaches after a third-party notified it.

190. Apria's "Security Monitoring and Response Policy" stated "[s]ystem must be in place to enable the detection and response to information technology system intrusion events."

191. Upon information and belief, Apria did not have this system in place.

192. If Apria had this system in place, Apria would have discovered the Data Breaches. Apria only discovered the Data Breaches after a third-party notified it.

193. Apria's "Data Security Policy" required Apria to label data into one of three security levels.

194. In practice, the Risk Assessments for 2020 and 2021 noted that Apria does not classify their data.

195. The "Data Security Policy" also stated that the I.T. Department would review servers, databases, mobile devices, backup media, and workstations to determine if encryption at rest is necessary.

196. In practice, none of Apria's data was encrypted at rest. This included ePHI and Personal Information.

197. If Apria encrypted its data, especially ePHI and Personal Information, Apria would have lessened the risk to Indiana consumers falling prey to identity deception or fraud.

198. Upon information and belief, Apria did not have an encryption mechanism for its data.

199. Apria's "External Party Security Policy" stated that all third parties working with ePHI must sign a Business Associate Agreement. Apria did not provide Plaintiff with any Business Associate Agreements.

VI. APPLICABILITY OF HIPAA TO APRIA

200. HIPAA regulates the use and disclosure of an individuals protected health information by health plans, health care clearinghouse and health care providers "who transmit[s] any health information in electronic form in connect with a transaction covered by this section" ("Covered Entities"). 45 C.F.R. § 160.102.

201. Generally, HIPAA privacy provisions are divided into three sections: the Privacy Rule, the Security Rule, and the Breach Notification Rule. See, 45 C.F.R. § 164 et seq.

202. The Privacy Rule applies to Covered Entities and establishes national standards to protect an individuals' medical records and other personal health information. 45 C.F.R. § 164 subparts A and E and 45 C.F.R. § 160.

203. The Security Rule establishes national standards to protect electronic personal health information that is created, received, used, or maintained by a covered entity. 45 C.F.R. § 164 subparts A and C and 45 C.F.R. § 160.

204. As a covered entity, Apria was required to comply with the HIPAA standards that govern the security and privacy of PHI and notification to patients in the event of a breach. *See* 45 C.F.R. Part 164.

205. During all times relevant to this complaint, Apria was regulated by and required to comply with the HIPAA Privacy Rule, Security Rule, and Breach Notification Rule.

206. The HIPAA Security Rule (45 C.F.R. Part 164, Subpart C) requires covered entities to ensure the confidentiality, integrity, and availability of all PHI that the covered entity creates, receives, maintains, or transmits and to protect against any reasonably anticipated threats to the security or integrity of such information. *See* 45 C.F.R § 164.306. To this end, the HIPAA Security Rule requires covered entities to employ appropriate administrative, physical, and technical

safeguards to maintain the security and integrity of PHI. *See* 45 C.F.R. §§ 164.308, 164.310, 164.312.

207. The HIPAA Breach Notification Rule (45 C.F.R. Part 164, Subpart D) requires covered entities to timely notify each individual whose unsecured PHI has been or is reasonably believed by the covered entity to have been accessed, acquired, used, or disclosed as a result of a breach. Notification must be provided "without unreasonable delay and ***in no case later than 60 calendar days*** after the discovery of a breach." 45 C.F.R. § 164.404(b) (emphasis added). "[A] breach shall be treated as discovered by a covered entity as of the first day on which such breach is known to the covered entity, or, by exercising reasonable diligence would have been known to the covered entity." 45 C.F.R. § 164.404(a)(2). Importantly, "Under this rule, the time period for breach notification begins when the incident is first known, not when the investigation of the incident is complete, even if it is initially unclear whether the incident constitutes a breach as defined in the rule." 78 Fed. Reg. 5648.

208. Finally, the HIPAA Privacy Rule (45 C.F.R. Part 164, Subpart E) prohibits covered entities from using or disclosing PHI, except as permitted by HIPAA.

209. The statute of limitations for violation of HIPAA is six years. 42 U.S. Code § 1320a–7a(c)(1) and 42 U.S.C. § 1320d-5(d)(7).

VII. CAUSES OF ACTION

COUNT I

Violations of HIPAA's Breach Notification Rule – 45 C.F.R. § 164.400, *et seq.*

210. Plaintiff incorporates herein by reference all preceding paragraphs as if fully set forth herein.

a. 45 C.F.R. § 164.404 – Failure to notify individuals without unreasonable delay.

211. Under the HIPAA Breach Notification Rule, Apria was required to provide direct notification to patients "without unreasonable delay and in no case later than 60 calendar days after the discovery of a breach." 45 C.F.R. § 164.404(b).

212. Apria discovered the Data Breaches on September 1, 2021, meaning Apria was required to provide direct notification to patients no later than November 1, 2021.

213. Apria did not start sending direct notice to patients until June 6, 2023, 644 days after the Data Breaches were first discovered.

214. Apria's notification to patients was unreasonably delayed and untimely, in violation of 45 C.F.R. § 164.404.

215. In the case of continuing violation of a provision, a separate violation occurs each day the covered entity or business associate is in violation of the provision. 45 C.F.R. § 160.406.

216. Apria's continued violations of 45 C.F.R. §164.404 *et seq.* resulted in at least 629 violations per person.

217. Apria's continued violations of 45 C.F.R. §164.404 *et seq.* resulted in at least 26,431,209 violations.

b. 45 C.F.R. § 164.406 – Failure to notify the media without unreasonable delay.

218. Under the HIPAA Breach Notification Rule, Apria was required to notify prominent media outlets "without unreasonable delay and in no case later than 60 calendar days after the discovery of a breach." 45 C.F.R. § 164.406(b).

219. Apria discovered the Data Breaches on September 1, 2021, meaning Apria was required to provide direct notification to the media no later than November 1, 2021.

220. Apria did not start sending direct notice to media until May 22, 2023, 629 days after the Data Breaches were first discovered.

221. Apria's notification to patients was unreasonably delayed and untimely, in violation of 45 C.F.R. § 164.406.

222. In the case of continuing violation of a provision, a separate violation occurs each day the covered entity or business associate is in violation of the provision. 45 C.F.R. § 160.406.

223. Apria's continued violations of 45 C.F.R. §164.406 *et seq.* resulted in at least 629 violations.

COUNT II

Violations of HIPAA's Security Rule – 45 C.F.R. § 164.308

224. Plaintiff incorporates herein by reference all preceding paragraphs as if fully set forth herein.

a. 45 C.F.R. § 164.308(a)(1)(ii)(B) – Risk Management

225. The Security Rule requires Apria to implement security management policies and procedures to prevent, detect, contain, and correct security violations. 45 C.F.R. § 164.308(a)(1).

226. The security management process must include risk analysis, risk management, sanction policy, and information system activity review. 45 C.F.R. § 164.308(a)(1)(ii).

227. Upon information and belief, Apria did not implement a risk management plan pursuant to 45 C.F.R. § 164.308(a)(1)(ii)(B).

228. A third-party conducted risk assessments on behalf of Apria in 2018, 2020, 2021, and 2022.

229. The risk assessments prior to the Data Breaches identified numerous risks that Apria did not remedy over the years.

230. For example, in the 2018 Risk Assessment, areas such as Privileged User Management, Threat and Vulnerability Management, Information Security Risk Management, ePHI Inventory and Risk Management, and Logging and Monitoring were listed as areas that needed to be worked on "to immediately reduce risk[.]"

231. The 2020 Risk Assessment identified similar risks and added additional risks.

232. Apria did not implement a risk management plan.

233. If Apria did implement a risk management plan, it is likely that Apria may have corrected its security issues and prevented the Data Breaches.

234. Dating back to at least May 2, 2018, Apria violated 45 C.F.R. § 164.308(a)(1)(ii)(B) in a continued and ongoing manner, including violating the HIPAA provision each day.

235. Dating back to at least May 2, 2018, Apria violated 45 C.F.R. § 164.308(a)(1)(ii)(B) at least 2,122 times.

b. 45 C.F.R. § 164.308(a)(1)(ii)(D) – Information System Activity Review

236. The Security Rule requires Apria to implement security management policies and procedures to prevent, detect, contain, and correct security violations. 45 C.F.R. § 164.308(a)(1).

237. The security management process must include risk analysis, risk management, sanction policy, and information system activity review. 45 C.F.R. § 164.308(a)(1)(ii).

238. During all times relevant to this Complaint, Apria did not implement an information system activity review pursuant to 45 C.F.R. § 164.308(a)(1)(ii)(D).

239. Apria failed to implement any security measures to reduce the risk of vulnerabilities.

240. The 2018 Risk Assessment states that Apria did not conduct periodic access reviews for all critical systems.

241. The 2018 Risk Assessment states that Apria needed to add logging requirements for at least multiple failed log-in attempts or new log-ins, admin authority changes, changes to roles and permissions, and data exports by privileged users.

242. Upon information and belief, Apria did not add the suggested logging requirements.

243. The Intruder used multiple accounts to log into Apria's system, make admin authority changes, make changes to roles and permissions, and grant privileged access to data exports.

244. If Apria made the recommended changes that were suggested in the 2018 Risk Assessment, it is likely that Apria could have prevented both Data Breaches.

245. By failing to implement a security management process, Apria has continuously violated C.F.R. 45 C.F.R. §164.308(a)(1)(ii)(D).

246. Dating back to at least May 2, 2018, Apria violated 45 C.F.R. § 164.308(a)(1)(ii)(D) in a continued and ongoing manner, including violating the HIPAA provision each day.

247. Dating back to at least May 2, 2018, Apria violated 45 C.F.R. § 164.308(a)(1)(ii)(D) at least 2,122 times.

c. 45 C.F.R. § 164.308(a)(3) – Failure to implement workforce security.

248. Apria is required to "[i]mplement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information, as provided under paragraph (a)(4) of this section, and to prevent those workforce members who do not have access under paragraph (a)(4) of this section from obtaining access to electronic protected health information." 45 C.F.R. § 160.308(a)(3)(i).

249. As part of appropriate access, Apria must assess whether it is reasonable and appropriate to "[i]mplement procedures to determine that the access of a workforce member to electronic protected health information is appropriate." 45 C.F.R. § 160.308(a)(3)(ii)(B).

250. If determined reasonable, Apria must implement workforce security safeguards.

251. If not reasonable, Apria must document why it is not reasonable and implement an equivalent alternative measure if reasonable and appropriate.

252. While on paper, Apria appears to have language addressing workforce security, it does not appear that Apria is following their workforce security policies and procedures.

253. Upon information and belief, Apria has not implemented the safeguards or the equivalent alternative.

254. The 2021 Risk Assessment identified that Apria performed privileged access reviews on only select applications.

255. The 2018 Risk Assessment identified that the approval and review process of privileged access was manual – resulting in errors.

256. The 2020 Risk Assessment identified that ePHI was accessible to all employees without a login.

257. Upon information and belief, Apria did not limit access to ePHI to employees who did not need access.

258. If this would have been implemented, it likely would have prevented the Data Breaches.

259. Dating back to at least May 2, 2018, Apria violated 45 C.F.R. § 164.308(a)(3)(i) in a continued and ongoing manner, including violating the HIPAA provision each day.

260. Dating back to at least May 2, 2018, Apria violated 45 C.F.R. § 164.308(a)(3)(i) at least 2,122 times.

d. 45 C.F.R. § 164.308(a)(5) – Failure to implement log-in monitoring.

261. Apria is required to implement security awareness and training. 45 C.F.R. § 164.30(a)(5).

262. As part of security awareness and training, Apria must assess whether it is reasonable and appropriate to implement procedures for monitoring log-in attempts and reporting discrepancies. 45 C.F.R. § 164.308(a)(5)(ii)(C).

263. If determined reasonable, Apria must implement procedures for monitoring log-in attempts and reporting discrepancies.

264. If not reasonable, Apria must document why it is not reasonable and implement an equivalent alternative measure if reasonable and appropriate.

265. Monitoring and logging were identified as a concern in Apria's 2018 Risk Assessment.

266. The 2018 Risk Assessment recommended that Apria "[d]efine minimum logging requirements for all critical systems. At minimum, include the following: Multiple failed log-in attempts or new log-ins; Admin authority changes; Changes to roles and permissions; Data exports by privileged user; Integrate critical systems with SIEM."

267. In the Forensic Report, CrowdStrike also noted that insufficient logging was an issue and recommended Apria make changes – indicating Apria did not change their logging practices after the 2018 Risk Assessment.

268. If this would have been implemented, it likely would have mitigated the harm caused by Data Breaches.

269. Dating back to at least May 2, 2018, Apria violated 45 C.F.R. § 164.308(a)(5)(ii)(C) in a continued and ongoing manner, including violating the HIPAA provision each day.

270. Dating back to at least May 2, 2018, Apria violated 45 C.F.R. § 164.308(a)(5)(ii)(C) at least 2,122 times.

e. 45 C.F.R. § 164.308(a)(6) – Failure to implement security incident procedures.

271. Apria is required to implement security incident procedures. 45 C.F.R. § 164.308(a)(6)(i).

272. As part of the security incident procedures, Apria is required to "[i]dentify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity . . . ; and document security incidents and their outcomes." 45 C.F.R. § 164.308(a)(6)(ii).

273. Apria's "Security Monitoring and Response Policy" during the discovery of the Data Breaches states "The information security incident management process will follow procedures developed by the [IT Security and Compliance Group]. The incident management process should be aligned with all third-party service provider procedures as appropriate."

274. The policy does not explain what procedures were created by the IT Security and Compliance Group or what procedures should be followed.

275. A policy to have a procedure is not a HIPAA compliant policy.

276. After notification from the FBI, Apria took 40 days to get the Intruder out of Apria's systems.

277. During this 40-day period, Apria continued to allow patients and consumers to purchase or sign-up for Apria's services even though Apria was aware of the potential dangers to patient ePHI and PII.

278. Apria did not notify patients about the Data Breaches until 629 days after Apria knew about the Data Breaches.

279. As such, Apria did not mitigate, to the extent practicable, harmful effects of security incidents that were known to Apria.

280. Dating back to at least May 2, 2018, Apria violated 45 C.F.R. § 164.308(a)(6) in a continued and ongoing manner, including violating the HIPAA provision each day.

281. Dating back to at least May 2, 2018, Apria violated 45 C.F.R. § 164.308(a)(6) at least 2,122 times.

f. 45 C.F.R. § 164.308(a)(8) – Failure to perform a periodic technical and nontechnical evaluation.

282. Apria is required to "[p]erform a periodic technical and nontechnical evaluation, based initially upon the standards implemented under this rule and, subsequently, in response to environmental or operational changes affecting the security of electronic protected health information, that establishes the extent to which a covered entity's or business associate's security policies and procedures meet the requirements of this subpart." 45 C.F.R. § 164.308(a)(8).

283. The Risk Assessments for 2020 and 2021 stated Apria did not review HIPAA applications as part of Apria's quarterly user access review process.

284. Further, while Apria has a policy requiring all IT Security Policies to be updated on an annual basis, the 2021 Risk Assessment states that the procedures and guidelines were not consistently updated.

285. By failing to perform technical and nontechnical evaluations, Apria has continuously violated 45 C.F.R. § 164.308(a)(8).

286. Dating back to at least May 2, 2018, Apria violated 45 C.F.R. § 164.308(a)(8) in a continued and ongoing manner, including violating the HIPAA provision each day.

287. Dating back to at least May 2, 2018, Apria violated 45 C.F.R. § 164.308(a)(8) at least 2,122 times.

g. 45 C.F.R. § 164.310(d)(2)(i) – Failure to implement device and media controls that addresses the final disposition of electronic protected health information and/or the hardware or electronic media on which it is stored.

288. Apria is required to implement device and media controls. 45 C.F.R. § 164.310(d)(1).

289. As part of the device and media controls, Apria is required to establish a policy that addresses the "final disposition of electronic protected health information and/or the hardware or electronic media on which it is stored." 45 C.F.R. § 164.310(d)(2)(i).

290. During all times relevant to this Complaint, Apria failed to follow their device and media controls policy and procedure, violating sections 45 C.F.R. § 164.310(d)(1), and 45 C.F.R. § 164.310(d)(2)(i).

291. The 2018 Risk Assessment recommended that Apria should conduct a review of ePHI as there was no documentation of where ePHI resided.

292. Further, the 2018 Risk Assessment recommended that Apria should limit the distribution and storage of ePHI.

293. The Risk Assessments for 2020 and 2021 also state that ePHI is pervasive across the organization in multiple databases and ePHI is copied into applications without proper notation or review.

294. If this would have been implemented, it likely would have mitigated the harm caused by the Data Breaches.

295. Dating back to at least May 2, 2018, Apria violated 45 C.F.R. § 164.310(d)(2)(i) in a continued and ongoing manner, including violating the HIPAA provision each day.

296. Dating back to at least May 2, 2018, Apria violated 45 C.F.R. § 164.310(d)(2)(i) at least 2,122 times.

h. 45 C.F.R. § 164.312(a) – Failure to implement access controls.

297. Apria is required to implement access controls. 45 C.F.R. § 164.312(a)(1).

298. As part of the access controls, Apria is required to assign a unique name and/or number for identifying and tracking user identity. 45 C.F.R. § 164.312(a)(2)(i).

299. During all times relevant to this Complaint, Apria failed to implement access controls which complied with requirements under 45 C.F.R. § 164.312(a)(1) and 45 C.F.R. § 164.312(a)(2)(i).

300. The 2020 Risk Assessment states that Apria's employees were able to access PHI without using log-in credentials.

301. Upon information and belief, Apria did not review which employees are able to access PHI.

302. During all times relevant to this Complaint, Apria did not use multi-factor authentication.

303. Upon information and belief, Apria did not require employees to change User IDs and passwords unless an employee's account was known or suspected to be compromised or if the password was "easily guessable."

304. By failing to implement device and media controls, Apria continuously committed violations of 45 C.F.R. § 164.312(a).

305. Dating back to at least May 2, 2018, Apria violated 45 C.F.R. § 164.312(a)in a continued and ongoing manner, including violating the HIPAA provision each day.

306. Dating back to at least May 2, 2018, Apria violated 45 C.F.R. § 164.312(a) at least 2,122 times.

i. 45 C.F.R. § 164.312(b) – Failure to implement audit controls.

307. Apria is required to "[i]mplement hardware, software, and/or procedural mechanism that record and examine activity in information systems that contain or use electronic protected health information." 45 C.F.R § 164.312(b).

308. During all times relevant to this Complaint, ePHI was pervasive across Apria's environment in multiple databases.

309. The Risk Assessments for 2020 and 2021 stated that Apria did not conduct a complete inventory of HIPAA databases.

310. Upon information and belief, Apria did not document ePHI coverage.

311. The 2018 Risk Assessment states that Apria did not document where ePHI resides in Apria's environment.

312. The Risk Assessments for 2020 and 2021 stated that ePHI was replicated in multiple systems without a notation that the data was ePHI.

313. If this would have been implemented, it likely would have mitigated the harm caused by the Data Breaches.

314. Dating back to at least May 2, 2018, Apria violated 45 C.F.R. § 164.312(b) in a continued and ongoing manner, including violating the HIPAA provision each day.

315. Dating back to at least May 2, 2018, Apria violated 45 C.F.R. § 164.312(b) at least 2,122 times.

j. 45 C.F.R. § 164.312(d) – Failure to implement person or entity authentication.

316. Apria is required to "[i]mplement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed."

317. During all times relevant to this Complaint, Apria did not use multi-factor authentication – even after receiving multiple recommendations to implement multi-factor authentication.

318. Upon information and belief, Apria has not implemented a procedure to verify that a person or entity seeking access to ePHI is the person or entity claimed to be.

319. Upon information and belief, Apria did not document who was accessing ePHI.

320. Upon information and belief, Apria does not verify if a person or entity seeking access is the correct person or entity.

321. If this would have been implemented, it likely would have prevented and/or mitigated the harm caused by the Data Breaches.

322. Dating back to at least May 2, 2018, Apria violated 45 C.F.R. § 164.312(d) in a continued and ongoing manner, including violating the HIPAA provision each day.

323. Dating back to at least May 2, 2018, Apria violated 45 C.F.R. § 164.312(d) at least 2,122 times.

k. 45 C.F.R. § 164.312(e)(2)(ii) – Failure to implement encryption mechanism.

324. Apria is required to "[i]mplement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network." 45 C.F.R. § 164.312(e)(1).

325. As part of the technical security measures, Apria must assess whether it is reasonable and appropriate to "[i]mplement a mechanism to encrypt electronic protected health information whenever deemed appropriate." 45 C.F.R. § 164.312(e)(2)(ii).

326. If determined reasonable, Apria must implement transmission security safeguards.

327. If not reasonable, Apria must document why it is not reasonable and implement an equivalent alternative measure if reasonable and appropriate.

328. During all times relevant to this Complaint, Apria's ePHI was not encrypted at rest.

329. While encryption is "addressable" under HIPAA, Apria did not document why it would be unreasonable to encrypt data at rest.

330. Based on the size and complexity of Apria, and the amount of patient information Apria stored, it would have been reasonable to implement transmission security and an encryption mechanism.

331. If this would have been implemented, it likely would have mitigated the harm caused by the Data Breaches.

332. Dating back to at least May 2, 2018, Apria violated 45 C.F.R. § 164.312(e)(2)(ii)) in a continued and ongoing manner, including violating the HIPAA provision each day.

333. Dating back to at least May 2, 2018, Apria violated 45 C.F.R. § 164.312(e)(1) at least 2,122 times.

COUNT III

Violations of HIPAA's Privacy Rule – 45 C.F.R. § 164.500

334. Plaintiff incorporates herein by reference all preceding paragraphs as if fully set forth herein.

a. 45 C.F.R. § 164.502 – Uses and Disclosures of Protected Health Information

335. As a covered entity, Apria was prohibited from disclosing PHI except as permitted by HIPAA. 45 C.F.R. § 164.502(a).

336. HIPAA defines "disclosure" as "the release, transfer, provision of access to, or divulging in any manner of information outside the entity holding the information." 45 C.F.R. § 160.103.

337. Apria's deficient security practices subjected the PHI of approximately 42,000 Indiana residents to disclosure during the Data Breaches.

338. The disclosures were not permitted under any HIPAA exception.

339. Apria violated 45 C.F.R. § 164.502 by making a disclosure or disclosures to an unauthorized third-party or parties.

340. Each disclosure was a separate violation of the Privacy Rule. 45 C.F.R. § 164.502 *et seq.*

341. Dating back to at least May 2, 2018, Apria violated 45 C.F.R. § 164.312(e)(2)(ii)) in a continued and ongoing manner, including violating the HIPAA provision each day.

342. Dating back to at least May 2, 2018, Apria violated 45 C.F.R. § 164.312(e)(1) at least 42,021 times.

b. 45 C.F.R. § 164.530(c)(1) – Safeguards.

343. As a covered entity, Apria "must have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 45 C.F.R. § 164.530(c)(1).

344. Apria did not have in place appropriate administrative, technical, and physical safeguards.

345. Because Apria did not have in place appropriate administrative, technical, and physical safeguards, Apria was unable to protect the privacy of PHI and ePHI.

346. Apria's deficient security practices subjected the PHI of approximately 42,000 Indiana residents to disclosure during the Data Breaches.

347. Dating back to at least May 2, 2018, Apria violated 45 C.F.R. § 164.530(c)(1) in a continued and ongoing manner, including violating the HIPAA provision each day.

348. Dating back to at least May 2, 2018, Apria violated 45 C.F.R. § 164.530(c)(1) at least 2,122 times.

COUNT IV

Violations of the Disclosure of Security Breach Act – Ind. Code 24-4.9

349. Plaintiff incorporates herein by reference all preceding paragraphs as if fully set forth herein.

350. Apria violated the Disclosure of Security Breach Act ("DSBA") by failing to disclose the Data Breaches without unreasonable delay. *See* Ind. Code § 24-4.9-3-1.

351. Apria was required to disclose the breach without unreasonable delay to Indiana residents whose "unencrypted personal information was or may have been acquired by an unauthorized person," if Apria knew or should have known "the unauthorized acquisition constituting the breach has resulted in or could result in identity deception (as defined in Ind. Code § 35-43-5-3.5), identity theft, or fraud affecting the Indiana resident." Ind. Code § 24-4.9-3-1(a)(1).

352. Apria was required to disclose the breach to the Office of the Indiana Attorney General without unreasonable delay. Ind. Code § 24-4.9-3-1(c).

353. As the breach impacted more than 1000 consumers, Apria was required to disclose to the credit reporting agencies without unreasonable delay. Ind. Code § 24-4.9-3-1(b).

354. The DSBA requires that a data base owner disclose a breach of security data. Ind. Code § 24-4.9-3-1.

355. The DSBA requires the data base owner ""shall make the disclosure or notification without unreasonable delay . . ." *See* Ind. Code § 24-4.9-3-3.

356. The DSBA defines "data base owner" as a "a person that owns or licenses computerized data that includes personal information." Ind. Code § 24-4.9-2-3.

357. Apria is and was a data base owner under Indiana law.

358. The DSBA defines "personal information" to include:

> (1) A Social Security number that is not encrypted or redacted; or
> (2) An individual's first and last manes, or first initial and last name, and one (1) or more of the following data elements that are not encrypted or redacted:
> (A) A driver's license number.
> (B) A state identification card number.
> (C) A credit card number.
> (D) A financial account number or debit card number in combination with a security code, password, or access code that would permit access to the person's account.

Ind. Code § 24-4.9-2-10.

359. The DSBA defines the "breach of security of data," as the "unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by a person." Ind. Code § 24-4.9-2-2.

360. Apria's breach in 2019 and breach in 2020 were breaches of security of data under Indiana law.

361. A delay is considered reasonable if the delay is:

1. necessary to restore the integrity of the computer system;
2. necessary to discover the scope of the breach; or
3. in response to a request from the attorney general or a law enforcement agency to delay disclosure because disclosure will:
   a. impede a criminal or civil investigation; or
   b. jeopardize national security.

Ind. Code § 24-4.9-3-3.

362. The categories of personal information exposed by the Data Breaches include full names, Social Security numbers, driver's license numbers, financial account information, and payment card information.

363. Apria's delay in disclosure was unreasonable.

364. The delay of at least 629 days was not necessary to restore the integrity of Apria's system.

365. The delay of at least 629 days was not necessary to discover the scope of the breach.

366. The delay of at least 629 number of days was not in response to law enforcement requesting a delay.

367. The DSBA also requires a data base owner to "implement and maintain reasonable procedures, including taking any appropriate corrective action, to protect and safeguard from unlawful use or disclosure any personal information of Indiana residents collected or maintained by the data base owner." Ind. Code § 24-4.9-3-3.5(c).

368. Apria violated the DSBA by failing to notify anyone of the Data Breaches until May 22, 2023 – 629 days after Apria first discovered the Data Breaches.

369. Apria violated the DSBA by failing to implement and maintain reasonable security procedures to protect and safeguard personal information of Hoosiers.

370. Apria is not exempt from the DSBA because Apria was not in compliance with HIPAA at the times relevant to this Complaint. *See* Ind. Code § 24-4.9-3-3.5(a).

COUNT V

Violations of Indiana Deceptive Consumer Sales Act – Ind. Code 24-5-0.5.

371. Plaintiff incorporates herein by reference all preceding paragraphs as if fully set forth herein.

372. The Deceptive Consumer Sales Act ("DCSA") regulates unfair, abusive, and/or deceptive acts, omissions and/or practices between suppliers and consumers engaging in consumer transactions. *See* Ind. Code § 24-5-0.5-3.

373. Under the DSCA, a "consumer transaction" includes services and other intangibles. Ind. Code § 24-5-0.5-2(a)(1).

374. As a supplier of health care services and supplies, Apria was and remains involved in consumer transactions in Indiana and therefore is a "supplier" as defined by Ind. Code § 24-5-0.5-2(a)(3).

375. The DCSA prohibits a supplier from committing "an unfair, abusive, or deceptive act, omission, or practice in connection with a consumer transaction . . . whether it occurs before, during, or after the transaction. An act, omission, or practice prohibited by this section includes both implicit and explicit misrepresentations." Ind. Code § 24-5-0.5-3(a).

376. It is a deceptive act under the DCSA to represent to consumers that the subject of a consumer transaction "has sponsorship, approval, performance, characteristics, accessories, uses, or benefits it does not have which the supplier knows or should reasonably know it does not have," or "is of a particular standard, quality, grade, style or model, if it is not and if the supplier knowns or should reasonably know that it is not." Ind. Code § 24-5-0.5-3(b)(1)-(2)

377. On its website and Notice of Privacy Practices, Apria represented to patients that they "maintain commercially reasonable security measures to protect the personal data we collect

and store from loss, misuse, destruction, or unauthorized access." Apria also implicitly represented that it was compliant with HIPAA and other applicable laws by stating: "Apria Healthcare LLC . . . [is] required by law to maintain the privacy of your protected health information, to provide you with Notice of our legal duties and privacy practices with respect to your PHI, and to notify you if a breach of your PHI occurs . . . ."

378. Further, Apria's website was active and allowing patients to sign up for Apria's programs or machines, fill prescriptions, and pay invoices while an active threat to Apria's environment was occurring.

379. Contrary to the above representations, Apria knowingly failed to implement and maintain reasonable security practices to protect Hoosier patients' PHI and personal information. Apria also knowingly failed to comply with HIPAA by failing to address the security issues flagged in Apria's 2018, 2020, and 2022 HIPAA Risk Assessments.

380. Apria explicitly and implicitly misrepresented that its systems were secure and compliant, when Apria knew that they were not.

381. Further, companies that accept credit cards and debit cards for payment must implement specific security measures, Payment Card Industry Data Security Standard ("PCI DSS"), as a minimum standard to protect payment information. *PCI Quick Reference Guide*, PCI Security Standards Council (2018) https://listings.pcisecuritystandards.org/documents/PCI_DSS-QRG-v3_2_1.pdf.

382. PCI DSS contains a list of twelve information security mandates. The basic requirements are: (1) Install and maintain a firewall configuration to protect cardholder data; (2) Do not use vendor-supplied defaults for system passwords and other security parameters; (3) Protect stored cardholder data; (4) Encrypt transmission of cardholder data across open, public

networks; (5) Protect all systems against malware and regularly update anti-virus software or programs; (6) Develop and maintain secure systems and applications; (7) Restrict access to cardholder data by business need to know; (8) Identify and authenticate access to system components; (9) Restrict physical access to cardholder data; (10) Track and monitor all access to network resources and cardholder data; (11) Regularly test security systems and processes; (12) Maintain a policy that addresses information security for all personnel. *Id.*

383. Upon information and belief, Apria does not follow the twelve security mandates.

384. As alleged herein, Apria has regularly engaged in a pattern or practice of unfair, abusive, and/or incurable deceptive acts, omissions, and/or practices affecting Indiana consumers in connection consumer transactions, in violation of Ind. Code 24-5-0.5-3(a) and (c).

385. Apria has committed unfair and deceptive acts, omissions, and practices violating Ind. Code § 24-5-0.5-3.

386. From at least April 5, 2019, Apria violated the DCSA in every consumer transaction with an Indiana consumer.

387. As Apria is currently not HIPAA or PCI-DSS compliant, Apria continues to violate the DCSA in every concurrent consumer transaction with an Indiana consumer.

CONSUMER INJURY

388. Consumers in the United States and in Indiana have suffered and will continue to suffer injury as a result of Defendant's violations of HIPAA and Indiana law. Absent injunctive relief by this Court, Defendant is likely to continue to injure consumers and harm the public interest.

RELIEF REQUESTED

WHEREFORE, Plaintiff requests that this Court:

1. Grant such other legal or equitable relief as this Honorable Court deems just and proper;

2. Enter judgment in favor of Plaintiff and against Defendant for the violations as alleged herein;

3. Grant all legal or equitable relief, as allowable by the laws described herein, including the specific relief below;

Relief Requested for Counts I, II, and III (HIPAA)

4. Award damages in favor of Plaintiff and against Defendant, regarding Counts I, II, and III;

5. Enjoin, as allowed by 42 U.S.C. 1320d-5(d)(1)(A), future violations 45 C.F.R. 164.302, *et seq.*;

6. Award damages to Plaintiff requiring Defendant pay up to $100 per violation, as allowed by 42 U.S.C. § 1320d-5(d)(2), for up to $25,000 per violation of an identical requirement per year, as allowed by 42 U.S.C. § 1320d-5(d)(2);

7. For continuous violations, award damages to Plaintiff requiring Defendant pay up to $100 per violation per day, as allowed by 42 U.S.C. § 1320d-5(d)(2) and 45 C.F.R. § 160.406.

Relief Requested for Count IV (DSBA)

8. Award damages in favor of Plaintiff and against Defendant, regarding Count IV;

9. Enjoin, as allowed by Ind. Code § 24-4.9-4-2(1), future violations of Ind. Code 24-4.8-3;

10. Award damages to Plaintiff requiring Defendant pay civil penalties up to $150,000, as allowed by Ind. Code § 24-4.9-4-2(2) and Ind. Code § 24-4.9-4-1(a), for the unreasonably delayed notification of Indiana residents, as required by Ind. Code § 24-4.9-3-1(a);

11. Award damages to Plaintiff requiring Defendant pay civil penalties up to $150,000, as allowed by Ind. Code § 24-4.9-4-2(2) and Ind. Code § 24-4.9-4-1(a), for the unreasonably delayed notification of consumer reporting agencies, as required by Ind. Code § 24-4.9-3-1(b);

12. Award damages to Plaintiff requiring Defendant pay civil penalties up to $150,000, as allowed by Ind. Code § 24-4.9-4-2(2) and Ind. Code § 24-4.9-4-1(a), for the unreasonably delayed notification of the Office of the Attorney General, as required by Ind. Code § 24-4.9-3-1(c);

13. Award damages to Plaintiff requiring Defendant to pay reasonable costs for Plaintiff's investigation and maintaining of this action, as allowed by Ind. Code § 24-4.9-4-2(4);

14. Enjoin, as allowed by Ind. Code § 24-4.9-3-3.5(f)(1), future violations of Ind. § Code 24-4.9-3-3.5;

15. Award damages to Plaintiff requiring Defendant to pay civil penalties up to $5,000 per deceptive act, as allowed by Ind. § Code 24-4.9-3-3.5(f)(2);

16. Award damages to Plaintiff requiring Defendant to pay reasonable costs for Plaintiff's investigation and maintaining of this action, as allowed by Ind. § Code 24-4.9-3-3.5(f)(3).

Relief Requested for Count V (DCSA)

17. Award damages in favor of Plaintiff and against Defendant, regarding Count V;

18. Enjoin, as allowed by Ind. Code § 24-5-0.5-4(c), Defendant from violating Ind. Code 24-5-0.5;

19. Award damages to Plaintiff requiring Defendant pay civil penalties up to $500 for each incurable deceptive act, as allowed by Ind. Code § 24-5-0.5-8;

20. Award damages to Plaintiff requiring Defendant pay civil penalties up to $5,000 for each violation of Ind. Code § 24-5-0.5-3. Ind. Code § 24-5-0.5-4(g);

21. Award damages to Plaintiff requiring Defendant pay triple damages for violations against a senior consumer, as allowed by Ind. Code § 24-5-0.5-4(c)(3);

22. Require Defendant to make payments of the money unlawfully received from aggrieved consumers to be held in escrow for distribution to aggrieved consumers, as allowed by Ind. Code § 24-5-0.5-4(c)(2);

23. Award damages to Plaintiff requiring Defendant to pay reasonable costs for Plaintiff's investigation and prosecution of this action, as allowed by Ind. Code § 24-5-0.5-4(c)(4);

24. Appoint a receiver, as allowed by Ind. Code § 24-5-0.5-4(c)(5);

25. Declare as void or limit the application of Defendant's contracts or clauses resulting from deceptive acts, as allowed by Ind. Code § 24-5-0.5-4(d);

26. Award damages to Plaintiff requiring Defendant's to pay restitution to aggrieved consumers, as allowed by Ind. Code § 24-5-0.5-4(d).

JURY DEMAND

27. Plaintiff hereby demands a trial by jury of all issues so triable pursuant to Rule 38 of the Federal Rules of Civil Procedure.

Dated: February 29, 2024

Respectfully Submitted,

THEODORE E. ROKITA
Attorney General for the State of Indiana

Indiana Bar No. 18857-49

/s/ Hannah E. Jones

HANNAH E. JONES
Deputy Attorney General
Indiana Bar No. 37950-53
Hannah.Jones@atg.in.gov

/s/ Joseph D. Yeoman

JOSEPH D. YEOMAN
Deputy Attorney General
Indiana Bar No. 35668-29
Joseph.Yeoman@atg.in.gov

/s/ Douglas S. Swetnam

DOUGLAS S. SWETNAM
Section Chief
Indiana Bar No. 15860-49
Douglas.Swetnam@atg.in.gov

302 West Washington Street
IGCS – 5th Floor
Indianapolis, IN 46204
(317) 232-1008 (Jones)
(317) 234-1912 (Yeoman)
(317) 232-6294 (Swetnam)
(317) 232-7979 (Fax)

Counsel for Plaintiff
STATE OF INDIANA