EXHIBIT A(2)

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF INDIANA
INDIANAPOLIS DIVISION

SUZANNE CUYLE, Individually And On Behalf Of All Others Similarly Situated, Plaintiff, v. APRIA HEALTHCARE, LLC, Defendant.	Case No. **CLASS ACTION COMPLAINT** **DEMAND FOR JURY TRIAL**

TABLE OF CONTENTS

1. Plaintiff Suzanne Cuyle ("Plaintiff"), individually and on behalf of all others similarly situated, brings this class action against Defendant Apria Healthcare LLC ("Apria" or "Defendant"), a Delaware Limited Liability Corporation, headquartered in Indianapolis, Indiana.

2. Plaintiff's allegations are based upon personal knowledge as to her own acts and upon information and belief as to all other matters alleged herein, including the investigation of counsel, publically available information, news articles, press releases, and additional analysis. Plaintiff believes that substantial evidentiary support will exist for the allegations set forth herein after a reasonable opportunity for discovery.

I. NATURE OF THE ACTION

3. Plaintiff brings this class action on behalf of herself and all persons whose personal information was compromised as a result of the data breaches announced by Apria on or about May 22, 2023 (the "Class").

4. Apria collects and maintains millions of records containing sensitive and personal information from its more than approximately two million patients, which it requires patients to provide in order to access Apria's services and products. The personal information includes, *inter alia*, personal, medical, health insurance, and financial information, as well as Social Security numbers (collectively, "PII").

5. On or about May 22, 2023, Apria announced that the PII for ***nearly 2 million*** Apria customers was accessed from its systems on or about April 5, 2019 to May 7, 2019 and on or about August 27, 2021 to October 10, 2021 by what it believes was an unauthorized third party (collectively the "Apria Breaches").

6. The Apria Breaches impact some of the nation's most vulnerable patients—those suffering from sleep, breathing, and/or or diabetic complications.

7. Plaintiff and Class members provided and entrusted their PII to Apria based on a reasonable expectation that Apria would safeguard that information and with the understanding that Apria would protect their PII against theft and not permit unauthorized access to, and/or misuse of, their data.

8. Apria promised to and had a duty to, but negligently failed to, implement, test, and maintain reasonable cyber-security measures to safeguard Plaintiff's and Class members' PII.

9. Although Apria assumed a duty to protect Plaintiff's and Class members' PII, contrary to the reasonable expectations of Apria patients, including Plaintiff and Class members, Apria failed to reasonably maintain the PII in a secure manner in breach of its implied agreements, and in violation of its legal duties and state laws.

10. In addition to Apria's failure to adequately implement, test, and maintain reasonable cyber-security measures to protect against the wrongful disclosure or compromise of the PII, Apria failed to timely detect and notify Plaintiff and Class members of the Apria Breaches in violation of applicable state data protection laws, including Indiana's data breach notification statute which requires "A person required to make a disclosure or notification . . . shall make the disclosure or notification without unreasonable delay, but not more than forty-five (45) days after the discovery of the breach." Ind. Code Ann. § 24-4.9-3-3.

11. Apria violated these statutes by failing to timely notify Plaintiff and Class members of the Apria Breaches.

12. Indeed, disclosure of the Apria Breaches took approximately four years from the date of the first 2019 hack, even though Apria identified that, *inter alia*, patient's personal debit

and credit card information was stolen.[1] Further still, two years after the 2019 hack, and two years before Plaintiff and Class members were notified, Apria was hacked yet again as a result of its failure to implement reasonable cyber-security measures.[2]

13. According to its own admission, Apria was notified of the Apria Breaches on September 1, 2021—yet it waited until May 22, 2023, or nearly two years later, to notify Plaintiff and Class members.[3] On information and belief, Apria unreasonably delayed disclosure in order to artificially bolster its valuation in its pending acquisition by Owens and Minor, consummated on March 29, 2022.[4]

14. Due to Apria's failure to properly safeguard Plaintiff's and Class members' PII and timely notify its users of the Apria Breaches, hackers may have had access to Plaintiff's and Class members' PII for years undetected, exposing Plaintiff and Class members to fraud, identity theft, financial harm, and to a heightened imminent risk of such harm in the future.

15. Especially alarming is the breadth of data that was stolen—personal, medical, health insurance, financial information, and Social Security numbers were accessed by hackers in the Apria Breaches. In fact, researchers at Purdue University recognize that data breaches of this type, where data like banking information was stolen, constitute the "worst imaginable" type of data breach.[5] Put simply, Plaintiff and Class members are now exposed to a "variety of crimes" based on Apria's failure to safeguard its PII.[6]

---

[1] Paulina Okunyte, *Apria Healthcare LLC Breach*, Cybernews (May 23, 2023), https://cybernews.com/news/apria-healthcare-llc-breach/.
[2] *Notice of Data Breach*, Apria, https://www.apria.com/notice-of-data-breach (last visited June 14, 2023).
[3] *Id.*
[4] Form 10-Q at 9, Owens and Minor, Inc., https://s202.q4cdn.com/322866865/files/doc_financials/2023/q1/65fc9b7f-875c-4ed9-8450-ee920d41d484.pdf (last visited June 14, 2023).
[5] *Top 10 Worst Data Breaches Of All Time*, Purdue University (Oct. 4, 2019), https://www.purdueglobal.edu/blog/information-technology/worst-data-breaches-infographic/.
[6] Karen Axelton, *What Do Hackers Do With Stolen Information*, Experian (Feb. 21, 2022), https://www.experian.com/blogs/ask-experian/what-do-hackers-do-with-stolen-information/.

16. Because Apria failed to take adequate and reasonable measures to ensure its computer systems were protected, failed to take available steps to prevent and stop the breach, failed to disclose the material fact that it did not have adequate computer systems and security practices to safeguard PII, and failed to provide timely and adequate notice of the Apria Breaches, Apria has caused substantial harm and injuries to consumers across the United States. Now that their PII has been released, Plaintiff and Class members must be super-vigilant and worry about being victimized for the rest of their lives.

17. Accordingly, Plaintiff, on behalf of herself and other members of the Class, asserts claims for negligence, negligence per se, unjust enrichment, breach of implied contract, invasion of privacy, violation of the Indiana Deceptive Consumer Sales Act, violation of the Washington Consumer Protection Act, violation of the Washington Personal Information—Notice of Security Breaches statute, and violation of the Washington Uniform Health Care Information Act.

II. PARTIES

18. Plaintiff Suzanne Cuyle resides in Lake Stevens, Washington and is a citizen of Washington. Prior to April 2019, Plaintiff provided her PII to Apria as part of the exchange for the purchase of Apria products. Plaintiff purchased home healthcare equipment using personal sensitive information, including, *inter alia*, her health insurance and medical records, Social Security number, and banking and credit card account information. Plaintiff entrusted her PII to Apria with the reasonable expectation and understanding that Apria would protect and safeguard that information from compromise, disclosure, and/or misuse by unauthorized users.

19. Defendant Apria Healthcare LLC is a Delaware limited liability corporation with its principal place of business located at 7353 Company Dr., Indianapolis, Indiana 46237. Apria is

"a leading provider of home medical equipment and clinical support" for over 25 years.[7] Apria boasts that it serves over 2.05 million patients within the sleep care, breathing problem, and diabetic patient population.[8] In March 2022, Owen and Minor announced that it closed its $1.6 billion deal for the acquisition of Apria.[9]

III. JURISDICTION AND VENUE

20. This Court has subject matter jurisdiction over this action pursuant to the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2), because this lawsuit has been brought as a class action on behalf of a proposed Class including millions of members, the aggregate claims of the putative Class members exceed $5 million exclusive of interest and costs, and one or more of the members of the putative Class are citizens of a different state than Apria.

21. This Court has jurisdiction over Apria because its principal place of business is located within this District, it conducts significant business in this District, has sufficient minimum contacts with this District, and much of the relevant conduct occurred in this District.

22. Venue is proper in this District pursuant to 28 U.S.C. § 1391(b) because: Apria resides within this District, transacts business, is found, and/or has agents in this District; a substantial part of the events giving rise to Plaintiff and the Class' claims arose in this District; and Apria has sufficient contacts with Indiana and this District.

IV. FACTUAL ALLEGATIONS

A. Apria Collects and Promises to Safeguard Plaintiff's and Class members' PII

23. Apria is a leading provider of home healthcare equipment and related services to approximately 2 million patients in the USA.

---

[7] Apria, https://www.apria.com/ (last visited June 14, 2023).
[8] *Id.*
[9] *Owens Minor Inc. Completes Acquisition of Apria Inc.*, Owens Minor (Mar. 29, 2022), https://www.owens-minor.com/news/owens-minor-inc-completes-acquisition-of-apria-inc/.

24. To purchase Apria's products, such as Positive Airway Pressure ("PAP") machines, chronic obstructive pulmonary disease ("COPD") ventilators, and Continuous Glucose Monitoring ("CGM") equipment, Apria requires its customers to provide, *inter alia*, their health insurance information, Social Security number, and debit and credit card information. Apria collects and maintains this PII on its network.

25. Plaintiff and Class members used Apria's products and services and provided their PII in exchange for those products and services with the understanding and reasonable expectation that Apria would protect and safeguard their PII from compromise, disclosure, and/or misuse by unauthorized users.

26. Although Apria assumed a duty to protect Plaintiff's and Class members' PII, contrary to the reasonable expectations of Apria users and Apria's assurances, Apria failed to reasonably maintain this information in a secure manner and failed to safeguard the PII from compromise, disclosure, and/or misuse by unauthorized parties, in violation of legal duties, and in violation of state laws.

B. The Apria Breaches and Apria's Failure to Timely Notify Plaintiff and Class members

27. On or about May 22, 2023, Apria announced on its website, that on September 1, 2021, Apria received a notification that it sustained a data breach by an unauthorized third party (the "Notice of Data Breach").[10]

28. The Apria Breaches included, *inter alia*, theft of account details including personal, medical, health insurance, financial information, and/or Social Security numbers. Apria has said that it believes that the Apria Breaches were perpetrated by an unauthorized third party.

[10] *Notice of Data Breach*, *supra* note 3.

29. The Notice of Data Breach stated in part:

> On September 1, 2021, Apria Healthcare LLC ("Apria") received a notification regarding access to select Apria systems by an unauthorized third party . . . Based on the investigation, it was determined that information . . . may have included personal, medical, health insurance or financial information, and in some limited cases, Social Security numbers.[11]

30. Upon information and belief, Apria learned of the Apria Breaches years before it made the actual announcement on May 22, 2023, and failed to notify its users, and the public, in an effort to artificially bolster its valuation in its pending acquisition by Owens and Minor.

31. While not publicly announcing the Apria Breaches until May 2023, according to its filing with the Office of the Maine Attorney General, the Apria Breaches occurred as early as April 2019.[12] More than 1.8 million persons were reported to be affected and the data reportedly stolen included: "Name or other personal identifier in combination with: **Financial Account Number or Credit/Debit Card Number (in combination with security code, access code, password or PIN for the account).**"[13] Importantly, Apria attested that the Apria Breaches were discovered on September 1, 2021 but that consumers were not notified until May 22, 2023.[14]

32. Despite possessing specific information concerning a massive breach, Apria misled the Class and the market concerning the security of sensitive information in its custody.

33. Apria's failure to safeguard its patients' PII is particularly egregious given its experience with prior data breaches. For example, in 2012 Apria was responsible for 65,700 patient records being stolen pursuant to a data breach.[15]

---

[11] *Id.*

[12] *Data Breach Notifications*, Maine Attorney General, https://apps.web.maine.gov/online/aeviewer/ME/40/bf218a4e-1ffd-4f14-a74d-3d34aec8d6c7.shtml (last visited June 14, 2023).

[13] *Id.*

[14] *Id.*

[15] Erin McCann, *Biggest Healthcare Data Breaches 2012*, Healthcare IT News (Dec. 12, 2022, 9:15 am) https://www.healthcareitnews.com/news/infographic-biggest-healthcare-data-breaches-2012.

34. Yet despite its prior experience with the consequences of a data breach for its customers, disclosure of the 2019 and 2021 Apria Breaches were not announced for nearly two years after the breaches were discovered, and four years after the first hack occurred in April 2019.

35. According to IBM, it takes on average 197 days for a company to detect a data breach and 69 days to contain a breach.[16]

36. Had Apria taken reasonable steps to protect and maintain the security of its network, it would have quickly detected the intrusion and could have alerted Plaintiff and members of the Class to the Apria Breaches promptly. Instead of detecting the data beach in the average 197 days it typically takes a company to do so, Apria took as much as 800 days.

37. Due to Apria's failure to properly safeguard the PII and timely discover and disclose the Apria Breaches, hackers had access to millions of Apria accounts for years undetected, exposing Plaintiff and Class members to fraud, identity theft, financial harm, and to a heightened continued risk of such harm in the future.

38. The Apria Breaches are a severe intrusion on highly confidential PII of Apria's medically vulnerable patients.[17]

C. Apria Had an Obligation to Protect Personal and Medical Information Under Federal and State Law and the Applicable Standard of Care

39. Defendant admits that it's a "business associate" covered by HIPAA, and as such is required to comply with the HIPAA Privacy Rule and Security Rule, 45 CFR Part 160 and Part 164.[18]

---

[16] Rob Sobers, *Data Breach Response Times: Trends and Tips*, Varonis (June 22, 2022) https://www.varonis.com/blog/data-breach-response-times#:~:text=The%20cost%20of%20a%20breach,costs%20businesses%20millions%20of%20dollars.

[17] *Apria Healthcare Breach Affects up To 1.8 Million Individuals*, HIPAA Journal (May 23, 2023) https://www.hipaajournal.com/apria-healthcare-breach-affects-up-to-1-8-million-individuals/.

[18] Apria, Inc., Schedule 14A, SEC (Feb. 22, 2022), https://www.sec.gov/Archives/edgar/data/1735803/000119312522048605/d271832ddefm14a.htm.

40. HIPAA's Privacy Rule, or *Standards for Privacy of Individually Identifiable Health Information*, establishes national standards for the protection of health information.

41. HIPAA's Security Rule, or Security Standards for the Protection of Electronic Protected Health Information, establishes a national set of security standards for protecting health information that is held or transferred in electronic form.

42. HIPAA requires Defendant to "comply with the applicable standards, implementation specifications, and requirements" of HIPAA "with respect to electronic protected health information."[19]

43. "Electronic protected health information" is "individually identifiable health information . . . that is (i) Transmitted by electronic media; (ii) Maintained in electronic media."[20]

44. HIPAA's Security Rule requires Defendant to "[p]rotect against any reasonably anticipated threats or hazards to the security or integrity of such information."[21]

45. HIPAA also requires Defendant to "review and modify the security measures implemented . . . as needed to continue provision of reasonable and appropriate protection of electronic protected health information."[22]

46. HIPAA also requires Defendant to "[i]mplement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights." 45 C.F.R. § 164.312(a)(1).

[19] 45 C.F.R. § 164.302.
[20] 45 C.F.R. § 160.103.
[21] 45 C.F.R. § 164.306(a).
[22] 45 C.F.R. § 164.306(e).

47. The Federal Trade Commission has found that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of the Federal Trade Commission Act. *See, e.g.*, *FTC v. Wyndham Worldwide Corp.*, 799 F. 3d 236 (3d Cir. 2015).

48. In addition to its obligations under federal and state laws, Defendant owed a duty to Plaintiff and Class members, whose PII was entrusted to Defendant, to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the PII in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. Defendant owed a duty to Plaintiff and Class members to provide reasonable security, including consistency with industry standards and requirements, and to ensure that its computer systems and networks, and the personnel responsible for them, adequately protected the PII of the Plaintiff and Class members.

49. Defendant owed a duty to Plaintiff and Class members, whose PII was entrusted to Defendant, to design, maintain, and test its computer systems to ensure that the PII in Defendant's possession was adequately secured and protected.

50. Defendant owed a duty to Plaintiff and Class members, whose PII was entrusted to Defendant, to create and implement reasonable data security practices and procedures to protect the PII in its possession, including adequately training its employees and others who accessed PII within its computer systems on how to adequately protect PII.

51. Defendant owed a duty to Plaintiff and Class members, whose PII was entrusted to Defendant, to implement processes that would detect a breach on its data security systems in a timely manner.

52. Defendant owed a duty to Plaintiff and Class members, whose PII was entrusted to Defendant, to act upon data security warnings and alerts in a timely fashion.

53. Defendant owed a duty to Plaintiff and Class members, whose PII was entrusted to Defendant, to disclose if its computer systems and data security practices were inadequate to safeguard individuals' PII from theft because such an inadequacy would be a material fact in the decision to entrust PII with Defendant.

54. Defendant owed a duty to Plaintiff and Class members, whose PII was entrusted to Defendant, to disclose, in a timely and accurate manner, when data breaches occurred.

55. Defendant owed a duty of care to Plaintiff and Class members because they were foreseeable and probable victims of any inadequate data security practices. Defendant collected Plaintiff's and Class members' PII directly from those individuals. Defendant knew that a breach of its data systems would cause Plaintiff and Class members to incur damages.

D. Apria Knew, or Should Have Known, That It Was Vulnerable to the Apria Breaches

56. Apria knew, or should have known, that its IT system and network were vulnerable to attacks by third-parties. Apria, however, failed to take corrective measures or implement proper safeguards to protect users' PII, even after Apria learned of prior security breaches.

57. Specifically, in August 2012, Apria was subject to a data breach that led to the theft of electronically protected health information of over 65,000 patients.[23] This prior breach should have been a wakeup call for Apria to address its network security. Instead, Apria failed to take reasonable steps to better secure its network with terrible consequences for its customers.

[23] *Apria Healthcare Inc., Privacy Manager Breach*, PrivacyRights.org, https://privacyrights.org/data-breaches/apria-healthcare-inc-privacy-manager-breach (last visited June 14, 2023).

58. Particularly in light of this prior security breach, Apria knew, or should have known, that its network was vulnerable to attacks by third-parties and should have taken steps to properly safeguard and protect customers' PII. Indeed, given Apria's previous data breach, it was foreseeable to Apria that the PII of Plaintiff and members of the Class was an attractive target for hackers and could be accessed if Apria did not implement, test, and maintain the proper cyber-security measures.

59. The Apria Breaches were the result of Apria's failure to abide by state and federal regulations, and industry standards and best practices, which required Apria to take reasonable steps to implement, test, and maintain adequate cyber-security measures to protect the PII of Plaintiff and Class members.

E. The Apria Breaches Have Harmed Plaintiff and Class members

60. Apria knowingly collected and maintained the PII of Plaintiff and members of the Class, and had a duty to exercise reasonable care in safeguarding, securing, and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties.

61. Plaintiff and members of the Class entrusted their PII to Apria with the understanding that Apria would safeguard the information from unauthorized access and/or use.

62. It was foreseeable that if Apria failed to take reasonable cyber-security measures, the PII of Plaintiff and members of the Class could be stolen, lost, misused, and/or disclosed to unauthorized users. Apria knew, or should have known, that its users' PII was an attractive target for cyber attackers, particularly in light of highly-publicized prior data breaches, and Apria failed to take reasonable precautions to safeguard the PII of its users, including Plaintiff and members of the Class.

63. By failing to implement necessary cyber-security measures to protect its users' PII, Apria departed from the reasonable standard of care and breached its duties to Plaintiff and members of the Class.

64. Plaintiff and millions of Class members have been seriously harmed by Apria's failure to implement proper cyber-security measures and safeguards to protect their PII. Sensitive and confidential information such as health insurance and medical records, Social Security numbers, and banking and credit card account information have been stolen and is now (and for the past two years, has been) in the hands of criminals to be bought, sold, or otherwise distributed for the purpose of misappropriating Plaintiff's and Class members' identities or property.

65. As a result of Apria's wrongful conduct, and delay in disclosing the Apria Breaches, Plaintiff and Class members face a serious threat of identity theft, fraud, drained bank accounts, and phishing. Fraudulent use of the information was possible for years before Apria provided notice of the Apria Breaches.

66. While Apria's Notice of Data Breach indicated that it will provide complimentary identity protection services, this offer comes years after the Apria Breaches occurred in which Plaintiff's and Class members' PII was susceptible to nefarious uses. Moreover, such services are not foolproof and do not guarantee that Plaintiff and Class members will not be exposed to continued fraudulent use of the PII which was compromised in the Apria Breaches.

67. Sontiq, a TransUnion company, reported that a data breach "is a security event in which sensitive, protected or confidential information is exposed, transmitted or stolen — making it ripe for exploitation by hackers for personal gain."[24] And data breaches "create the ripe

[24] Jim Van Dyke, *Data Breaches: Fuel for the Identity Theft and Fraud Fire*, Sontiq (Feb. 3, 2022) https://www.sontiq.com/resources/what-is-a-data-breach/.

environment for identity theft scams and fraud, which totaled $56 billion in 2020 in the U.S. alone."[25]

68. In addition, due to the breadth of the information stolen in the Apria Breaches, the financial accounts of Plaintiff and Class members have been, and remain, vulnerable to fraud or identity theft.

69. Defendant breached its duty to Plaintiff and Class members to create and implement reasonable data security practices and procedure to protect PII in its possession.

70. Defendant breached its duty to Plaintiff and Class members to implement processes that would detect a breach of its computer systems in a timely manner.

71. Defendant breached its duty to Plaintiff and Class members to disclose the material fact that Defendant's computer systems and data security practices were inadequate to safeguard their PII. Had Defendant disclosed to Plaintiff and Class members that its computer systems and data security practices were inadequate to safeguard PII, Plaintiff and Class members would not have allowed their PII to be entrusted to Defendant.

72. Defendant breached its duty to Plaintiff and Class members to disclose in a timely and accurate manner that the Apria Breaches had occurred. Defendant failed to notify potentially affected customers for nearly two years after Defendant claims it discovered the breach. As a result, Plaintiff and Class members were not notified of the Apria Breaches until May 22, 2023 or later.

73. Defendant's failure to notify Plaintiff and Class members of the Apria Breaches in a timely and accurate manner allowed the cyber attackers to begin to use the PII before Plaintiff and Class members had an opportunity to take steps to protect themselves.

---

[25] *Id.*

74. As a direct and proximate result of Apria's breach of its legal duties and implied contracts with Plaintiff and members of the Class, and violation of HIPAA, state data protection and consumer protection laws, Plaintiff and members of the Class have suffered damages, and will continue to suffer damages, including, but not limited to: (l) the loss of the opportunity to control how their PII is used; (2) the diminution in the value and/or use of their PII entrusted to Apria with the understanding that Apria would safeguard their PII against theft and not allow access and misuse of their PII by others; (3) the compromise, disclosure, theft, and/or misuse of their PII; (4) out-of-pocket costs associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of PII; (5) lost opportunity costs associated with effort expended and the loss of productivity from addressing and attempting to mitigate the actual and future consequences of the Apria Breaches, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft and/or PII misuse; (6) the continued risk to their PII, which remains in Apria's possession and is subject to further breaches so long as Apria fails to undertake appropriate and adequate measures to protect the PII in its possession; and (7) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Apria Breaches.

75. As a further result of Apria's failure to provide adequate safeguards for the PII and failure to timely notify Plaintiff and members of the Class that their PII was compromised, Plaintiff and members of the Class have been harmed in that they were unable to take the necessary precautions to mitigate their damages by preventing identity theft and/or fraud.

V. CLASS ACTION ALLEGATIONS

76. Plaintiff brings this action pursuant to Federal Rule of Civil Procedure 23 on behalf of the following Class and Sub-Class:

> **Nationwide Class**: All persons whose personal information was compromised as a result of the data breaches announced by Apria on or about May 22, 2023 (the "Nationwide Class" or "Class").
>
> **Washington Sub-Class**: All residents of Washington whose personal information was compromised as a result of the data breaches announced by Apria on or about May 22, 2023 (the "Washington Sub-Class" or "Sub-Class").[26]

77. Excluded from the proposed Class and Sub-Class are Apria, as well as its agents, officers, directors and their families, as well as its parent companies, subsidiaries, and affiliates. Any judicial officer assigned to this case is also excluded. Plaintiff reserves the right to revise the definition of the Class and Sub-Class based upon subsequently discovered information.

78. This action is brought and may be properly maintained as a class action under Federal Rules of Civil Procedure 23(a) and 23(b)(3).

79. The Classes are so numerous that joinder of all members is impracticable. Plaintiff believes that there are millions of proposed Class members throughout the United States.

80. Common questions of law and fact exist as to all members of the Classes and predominate over any issues solely affecting individual members of the Classes. The common questions of law and fact include, but are not limited to:

a) Whether Defendant failed to adequately safeguard Plaintiff's and the Classes' PII;

b) Whether Defendant failed to protect Plaintiff's and the Classes' PII, as promised;

c) Whether Defendant's computer systems and data security practices used to protect Plaintiff's and the Classes' PII violated HIPAA, federal, state and local laws, or Defendant's duties;

d) Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard Plaintiff's and the Classes' PII properly and/or as promised;

[26] The Nationwide Class and the Washington Sub-Class are collectively referred to as "the Classes."

e) Whether Defendant violated the consumer protection statutes, data breach notification statutes, and state and federal medical privacy statutes applicable to Plaintiff and each of the Classes;

f) Whether Defendant failed to notify Plaintiff and members of the Classes about the Apria Breaches as soon as practical and without delay after the Apria Breaches were discovered;

g) Whether Defendant acted negligently in failing to safeguard Plaintiff's and the Classes' PII;

h) Whether Defendant entered into implied contracts with Plaintiff and the members of the each of the Classes that included promises requiring Defendant to protect the confidentiality of Plaintiff's PII and have reasonable security measures;

i) Whether Defendant's conduct described herein constitutes a breach of its implied contracts with Plaintiff and the members of each of the Classes;

j) Whether Defendant should be unjustly enriched by retaining money paid by Plaintiff and Class members for products and services, which included money that should have been used by Defendant to provide reasonable data security and safeguards;

k) Whether Plaintiff and the members of the Classes are entitled to damages as a result of Defendant's wrongful conduct;

l) Whether Plaintiff and the members of the Classes are entitled to restitution as a result of Defendant's wrongful conduct; and

m) What equitable relief is appropriate to redress Defendant's wrongful conduct.

81. Plaintiff's claims are typical of the claims of the Classes. As alleged herein, Plaintiff and members of the Classes all sustained damages arising out of the same course of unlawful conduct by Defendant.

82. Plaintiff is willing and prepared to serve the Classes in a representative capacity with all of the obligations and duties material thereto. Plaintiff will fairly and adequately protect the interests of the Classes and has no interests adverse to, or which conflict with, the interests of the other members of the Classes.

83. Plaintiff's interests are co-extensive with, and not antagonistic to, those of the absent members of the Classes. Plaintiff will undertake to represent and protect the interests of the absent members of the Classes.

84. Plaintiff has engaged the services of the undersigned counsel. Counsel is experienced in complex litigation, will adequately prosecute this action, and will assert and protect the rights of, and otherwise represent, Plaintiff and the absent members of the Classes.

85. A class action is superior to all other available methods for the fair and efficient adjudication of this controversy. Plaintiff knows of no difficulty to be encountered in the management of this litigation that would preclude its maintenance as a class action.

86. Class action status is warranted under Rule 23(b)(3) because questions of law or fact common to the members of the Classes predominate over any questions affecting only individual members, and a class action is superior to other available methods for the fair and efficient adjudication of this controversy.

87. The interest of members of the Classes in individually controlling the prosecution of separate actions is theoretical and not practical. Prosecution of the action through multiple representatives would be objectionable and Plaintiff anticipates no difficulty in the management of this matter as a class action.

VI. CLAIMS

FIRST CLAIM
NEGLIGENCE
(On behalf of the Nationwide Class)

88. Plaintiff incorporates and realleges the allegations in the preceding paragraphs as if fully set forth herein.

89. Plaintiff brings this claim on behalf of herself and the Nationwide Class.

90. Apria knowingly collected and maintained the PII of Plaintiff and members of the Class, and had a duty to exercise reasonable care in safeguarding, securing, and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties.

91. Defendant knew, or should have known, of the risks inherent in collecting and storing the PII of Plaintiff and Class members.

92. As described above, Defendant owed duties of care to Plaintiff and Class members whose PII had been entrusted with Defendant.

93. Apria owed Plaintiff and members of the Class a duty to take reasonable steps to maintain and protect against any dangers presented by cyber-attackers to Plaintiff's and members of the Class' PII. This duty included, among other things, maintaining and testing its cyber-security systems, taking other reasonable security measures to protect and adequately secure PII of Plaintiff and members of the Class from unauthorized access, and taking reasonable steps to ensure that hackers did not compromise the systems and/or gain access to its users' PII.

94. Apria owed a duty of care to Plaintiff and members of the Class because it was foreseeable that it would be harmed by Apria's inadequate cyber-security practices. By failing to implement necessary measures to protect its users' PII, Apria departed from the reasonable standard of care and breached its duties to Plaintiff and members of the Class.

95. It was foreseeable that if Apria did not take reasonable security measures, the PII of Plaintiff and members of the Class could be stolen, lost, misused, and/or disclosed to unauthorized users. Apria knew or should have known that its users' PII was an attractive target for cyber attackers, particularly in light of prior data breaches, and Apria failed to take reasonable precautions to safeguard the PII of its users, including Plaintiff and members of the Class.

96. Defendant breached its duties to Plaintiff and Class members by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and Class members' PII.

97. Defendant acted with wanton disregard for the security of Plaintiff's and Class members' PII. Defendant knew or should have known that it had inadequate computer systems and data security practices to safeguard such information, and Defendant knew or should have known that hackers were attempting to access the PII in computer systems, such as theirs.

98. As a direct and proximate result of Apria's failure to exercise reasonable care and deploy reasonable cyber-security measures, the PII of Plaintiff and members of the Class was accessed by cyber-attackers and can be used to commit identity theft and/or fraud.

99. But for Apria's failure to implement and maintain adequate cyber-security measures to protect Plaintiff's and member of the Class' PII, Plaintiff's and members of the Class' PII would not have been compromised, stolen, and/or disclosed to unauthorized users, Plaintiff and members of the Class would not have been injured, and Plaintiff and members of the Class would not be at a heightened future risk of identity theft and/or fraud.

100. Apria had and continues to have a duty to timely disclose that Plaintiff's and members of the Class' PII within its possession might have been compromised, lost, stolen, misused, and/or disclosed to unauthorized parties and precisely the types of information compromised.

101. Apria unlawfully breached its duty to timely disclose to Plaintiff and members of the Class the fact that their PII was compromised, lost, stolen, misused, and/or disclosed to unauthorized parties and precisely the type of information compromised.

102. As a result of Apria's negligence, Plaintiff and members of the Class have suffered damages including, but not limited to: (l) the loss of the opportunity to control how their PII is used; (2) the diminution in the value and/or use of their PII entrusted to Apria with the understanding that Apria would safeguard their PII against theft and not allow access and misuse of their PII by others; (3) the compromise, disclosure, theft, and/or misuse of their PII; (4) out-of-pocket costs associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of PII; (5) lost opportunity costs associated with effort expended and the loss of productivity from addressing and attempting to mitigate the actual and future consequences of the Apria Breaches, including, but not limited to, efforts spent researching how to prevent, detect, contest, and recover from identity theft and/or PII misuse; (6) the continued risk to their PII, which remains in Apria's possession and is subject to further breaches so long as Apria fails to undertake appropriate and adequate measures to protect the PII in its possession; and (7) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Apria Breaches.

103. As a further result of Apria's negligence in failing to timely notify Plaintiff and members of the Class that their PII was compromised, Plaintiff and members of the Class have been harmed in that they have been unable to take the necessary precautions to mitigate their damages by preventing future identity theft and/or fraud.

104. As a direct and proximate result of Defendant's negligent conduct Plaintiff and members of the Class have suffered injury and are entitled to damages.

SECOND CLAIM
NEGLIGENCE PER SE
(On behalf of the Nationwide Class)

105. Plaintiff incorporates and realleges the allegations in the preceding paragraphs as if fully set forth herein.

106. Plaintiff brings this claim on behalf of herself and the Nationwide Class.

107. Pursuant to the Federal Trade Commission Act (15 U.S.C. § 45), Defendant had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiff's and Class members' PII.

108. Pursuant to HIPAA's Privacy Rule and Security Rule, Defendant had a duty to implement reasonable safeguards to protect Plaintiff's and Class members' PII.

109. Defendant breached its duties to Plaintiff and Class members under the Federal Trade Commission Act and HIPAA, by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and Class members' PII.

110. Defendant's failure to comply with applicable laws and regulations constitutes negligence per se.

111. But for Defendant's wrongful and negligent breach of its duties owed to Plaintiff and Class members, Plaintiff and Class members would not have been injured.

112. The injury and harm suffered by Plaintiff and Class members was the reasonably foreseeable result of Defendant's breach of its duties. Defendant knew or should have known that it was failing to meet its duties, and that Defendant's breach would cause Plaintiff and Class members to experience the foreseeable harms associated with the exposure of their PII.

113. As a direct and proximate result of Apria's breached duties to Plaintiff and Class members under the Federal Trade Commission Act and HIPAA, Plaintiff and members of the Class have suffered damages and will continue to suffer damages including, but not limited to: (l) the loss of the opportunity to control how their PII is used; (2) the diminution in the value and/or use of their PII entrusted to Apria with the understanding that Apria would safeguard their PII against theft and not allow access and misuse of their PII by others; (3) the compromise, disclosure,

theft, and/or misuse of their PII; (4) out-of-pocket costs associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of PII; (5) lost opportunity costs associated with effort expended and the loss of productivity from addressing and attempting to mitigate the actual and future consequences of the Apria Breaches, including but not limited to, efforts spent researching how to prevent, detect, contest, and recover from identity theft and/or PII misuse; (6) the continued risk to their PII, which remains in Apria's possession and is subject to further breaches so long as Apria fails to undertake appropriate and adequate measures to protect the PII in its possession; and (7) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Apria Breaches.

THIRD CLAIM
BREACH OF IMPLIED CONTRACT
(On behalf of the Nationwide Class)

114. Plaintiff incorporates and realleges the allegations in the preceding paragraphs as if fully set forth herein.

115. Plaintiff brings this claim on behalf of herself and the Nationwide Class.

116. Plaintiff and members of the Class entered into implied contracts with Apria under which Plaintiff and members of the Class provided PII in order to receive Apria's goods and services with the understanding that Apria agreed to safeguard and protect that PII.

117. Plaintiff and members of the Class would not have provided their PII to Apria without the understanding that Apria would protect and safeguard their PII.

118. Apria breached its implied contracts with Plaintiff and Class members by failing to safeguard the PII of Plaintiff and members of the Class and by permitting the compromise and/or disclosure of that PII to unauthorized users.

119. As a direct and proximate result of Apria's breach of its implied contracts with Plaintiff and members of the Class, Plaintiff and members of the Class have suffered damages and will continue to suffer damages including, but not limited to: (l) the loss of the opportunity to control how their PII is used; (2) the diminution in the value and/or use of their PII entrusted to Apria with the understanding that Apria would safeguard their PII against theft and not allow access and misuse of their PII by others; (3) the compromise, disclosure, theft and/or misuse of their PII; (4) out-of-pocket costs associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of PII; (5) lost opportunity costs associated with effort expended and the loss of productivity from addressing and attempting to mitigate the actual and future consequences of the Apria Breaches, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft and/or PII misuse; (6) the continued risk to their PII, which remains in Apria's possession and is subject to further breaches so long as Apria fails to undertake appropriate and adequate measures to protect the PII in its possession; and (7) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Apria Breaches.

FOURTH CLAIM
UNJUST ENRICHMENT
(On behalf of the Nationwide Class)

120. Plaintiff incorporates and realleges the allegations in the preceding paragraphs as if fully set forth herein.

121. Plaintiff brings this claim on behalf of herself and the Nationwide Class.

122. Plaintiff and Class members conferred a monetary benefit on Defendant. Defendant received and retained money belonging to Plaintiff and Class members in the form of profits from the provision of Defendant's goods and services.

123. Defendant appreciated or had knowledge of the benefits conferred on them by Plaintiff and Class members.

124. The money that Plaintiff and Class members paid indirectly to Defendant were supposed to be used by Defendant, in part, to pay for the administrative costs of reasonable data privacy and security practices and procedures.

125. As a result of Defendant's conduct, Plaintiff and Class members suffered damages in an amount equal to the difference in value between health care goods and services with the reasonable data privacy and security practices and procedures that Plaintiff and Class members paid for, and the inadequate health care good and services without reasonable data privacy and security practices and procedures that it received.

126. Under principals of equity and good conscience, Defendant should not be permitted to retain the money belonging to Plaintiff and Class members paid to Defendant but where Defendant failed to implement (or adequately implement) the data privacy and security practices and procedures that Plaintiff and Class members paid for and that were otherwise mandated by HIPAA regulations, federal, state, and local laws and industry standards.

127. Defendant should be compelled to disgorge into a common fund for the benefit of Plaintiff and Class members all unlawful or inequitable proceeds received by Defendant.

128. A constructive trust should be imposed on all unlawful or inequitable sums received by Defendant traceable to Plaintiff and Class members.

FIFTH CLAIM
INDIANA DECEPTIVE CONSUMER SALES ACT,
IND. CODE ANN. § 24-5-0.5-3
(On behalf of the Nationwide Class)

129. Plaintiff incorporates and realleges the allegations in the preceding paragraphs as if fully set forth herein.

130. Plaintiff brings this claim on behalf of herself and the Nationwide Class.

131. Defendant is a "supplier" who engaged in deceptive, unfair, and unlawful trade acts or practices in the conduct of "consumer transactions" pertaining to the purchase and sale of home healthcare equipment in Indiana for personal, family, and/or household purposes to the Nationwide Class, in violation of Ind. Code Ann. § 24-5-0.5-3, including but not limited to the following:

a) Defendant omitted, suppressed, and concealed the material fact of the inadequacy of the privacy and security protections for Plaintiff and Class members' PII.

b) Defendant engaged in deceptive, unfair, and unlawful trade acts or practices by failing to maintain the privacy and security of Plaintiff and Class members' PII, in violation of duties imposed by and public policies reflected in applicable federal and state laws, resulting in the Apria Breaches. These unfair acts and practices violated duties imposed by laws including the Federal Trade Commission Act (15 U.S.C. § 45), HIPAA (42 U.S.C. § 1302d *et seq*.), and Indiana's data breach statute (Ind. Code Ind. Code Ann. § 24-4.9-3-3.5).

c) Defendant engaged in deceptive, unfair, and unlawful trade acts or practices by failing to disclose the Apria Breaches to Class members in a timely and accurate manner, contrary to the duties imposed by Ind. Code Ann. § 24-4.9-3.5.

132. As a direct and proximate result of Defendant's deceptive trade practices, Class members suffered injuries, including the loss of their legally protected interest in the confidentiality and privacy of their PII, and damages.

133. The above unfair and deceptive practices and acts by Defendant were done as part of a scheme, artifice, or device with intent to defraud or mislead and constitute incurable deceptive acts under Ind. Code Ann. § 24-5-0.5-1 *et seq*.

134. Among other acts, Defendant unreasonably delayed disclosure of the Apria Breaches in violation of its statutory and common law duties in order to artificially bolster its valuation in connection with its acquisition by Owens and Minor.

135. Defendant knew or should have known that its computer systems and data security practices were inadequate to safeguard Plaintiff and Class members' PII and that risk of a data breach or theft was highly likely.

136. Class members seek relief under Ind. Code Ann. § 24-5-0.5-4, including, but not limited to damages, restitution, penalties, injunctive relief, and/or attorneys' fees and costs. Senior members of the Class injured by Defendant's unfair and deceptive trade practices also seek treble damages, pursuant to Ind. Code Ann. § 24-5-0.5-4(i).

SIXTH CLAIM
INTRUSION UPON SECLUSION/INVASION OF PRIVACY
(On behalf of the Nationwide Class)

137. Plaintiff incorporates and realleges the allegations in the preceding paragraphs as if fully set forth herein.

138. Plaintiff brings this claim on behalf of herself and the Nationwide Class.

139. Plaintiff's and Class members' PII included information private in nature (e.g., health insurance and medical records, Social Security numbers, and banking and credit card account information). Plaintiff's and Class members' PII is information not of legitimate concern to the public.

140. Plaintiff and Class members had a legitimate and reasonable expectation of privacy with respect to their PII and were accordingly entitled to the protection of this information against disclosure to unauthorized third parties.

141. Defendant owed a duty to patients and customers, including Plaintiff and Class members, to keep their PII confidential.

142. The unauthorized release of PII, especially the type related to personal health and financial information, is highly offensive to a reasonable person.

143. The intrusion was into a place or thing, which was private and is entitled to be private. Plaintiff and Class members disclosed their PII to Defendant as part of its use of Defendant's services and/or purchase of Defendant's products, but privately, with the intention that the PII would be kept confidential and protected from unauthorized disclosure. Plaintiff and Class members were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization.

144. The Apria Breaches constitute an intentional interference with Plaintiff and Class members' interest in solitude or seclusion, either as to their persons or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person. Unauthorized third parties may have had access to Plaintiff's and Class members' PII for years undetected, exposing Plaintiff and Class members to fraud, identity theft, financial harm, and to a heightened imminent risk of such harm in the future. Additionally, Plaintiff and Class members suffer from the ongoing risk of further unauthorized disclosure of their PII.

145. Defendant acted with a knowing state of mind when it permitted the Apria Breaches because it knew its information security practices were inadequate and would likely result in a data breach such as the one that harmed Plaintiff and Class members.

146. Acting with knowledge, Defendant had notice and knew that its inadequate cybersecurity practices would cause injury to Plaintiff and Class members.

147. Defendant's unlawful invasions of privacy damaged Plaintiff and Class members. As a direct and proximate result of Defendant's unlawful invasion of privacy, Plaintiff and Class members suffered significant anxiety and distress, and their reasonable expectations of privacy were frustrated and defeated. Plaintiff and the Class seek actual and nominal damages for these invasions of privacy.

SEVENTH CLAIM
WASHINGTON CONSUMER PROTECTION ACT,
WASH. REV. CODE § 19.86.020, *et seq.*
(On behalf of the Washington Sub-Class)

148. Plaintiff incorporates and realleges the allegations in the preceding paragraphs as if fully set forth herein.

149. Plaintiff brings this claim on behalf of herself and the Washington Sub-Class.

150. Defendant engaged in deceptive, unfair, and unlawful trade acts or practices in the conduct of trade or commerce, in violation of Wash. Rev. Code §19.86.020, including but not limited to the following:

151. Defendant omitted, suppressed, and concealed the material fact of the inadequacy of the privacy and security protections for Plaintiff's and Washington Sub-Class members' PII.

152. Defendant engaged in deceptive, unfair, and unlawful trade acts or practices by failing to maintain the privacy and security of Plaintiff's Washington Sub-Class members' PII, in violation of duties imposed by and public policies reflected in applicable federal and state laws, resulting in the Apria Breaches. These unfair acts and practices violated duties imposed by laws including Federal Trade Commission Act (15 U.S.C. § 45), HIPAA (42 U.S.C. § 1302d *et seq*.),

and the Washington regulations pertaining to Privacy of Consumer Financial and Health Information (WAC 284-04-300).

153. Defendant engaged in deceptive, unfair, and unlawful trade acts or practices by failing to disclose the Apria Breaches to Plaintiff and Washington Sub-Class members in a timely and accurate manner, contrary to the duties imposed by Wash. Rev. Code § 19.255.010(1).

154. Defendant engaged in deceptive, unfair, and unlawful trade acts or practices by failing to take proper action following the Apria Breaches to enact adequate privacy and security measures and protect Plaintiff's and Washington Sub-Class members' PII from further unauthorized disclosure, release, data breaches, and theft.

155. As a direct and proximate result of Defendant's deceptive trade practices, Plaintiff and Washington Sub-Class members suffered injury and/or damages.

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

157. Defendant knew or should have known that its computer systems and data security practices were inadequate to safeguard Plaintiff's and Washington Sub-Class members' PII and that risk of a data breach or theft was highly likely. Defendant's actions in engaging in the above-named unfair practices and deceptive acts were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of members of the Washington Sub-Class.

158. Plaintiff and Washington Sub-Class members seek relief under Wash. Rev. Code § 19.86.090, including, but not limited to, actual damages, treble damages, injunctive relief, and attorneys' fees and costs.

EIGHTH CLAIM
PERSONAL INFORMATION--NOTICE OF SECURITY BREACHES,
WASH. REV. CODE ANN. § 19.255.010(1), *et seq.*
(On behalf of the Washington Sub-Class)

159. Plaintiff incorporates and realleges the allegations in the preceding paragraphs as if fully set forth herein.

160. Plaintiff brings this claim on behalf of herself and the Washington Sub-Class.

161. Defendant is required to accurately notify Plaintiff and Washington Sub-Class members following discovery or notification of the breach of its data security system (if personal information was, or is reasonably believed to have been, acquired by an unauthorized person and the personal information was not secured) "in the most expedient time possible, without unreasonable delay, and no more than thirty calendar days after the breach was discovered" under Wash. Rev. Code Ann. § 19.255.010(8).

162. Defendant is a business that owns or licenses computerized data that includes personal information as defined by Wash. Rev. Code Ann. § 19.255.005(2)(a).

163. Plaintiff's and Washington Sub-Class members' PII (e.g., health insurance and medical records, Social Security numbers, and banking and credit card account information) includes personal information as covered under Wash. Rev. Code Ann. § 19.255.005(2)(a) (including e.g., Social Security number, account number or credit or debit card number, full date of birth, Health insurance policy number or health insurance identification number, medical history).

164. Because Defendant discovered a breach of its security system (in which personal information was, or is reasonably believed to have been, acquired by an unauthorized person and the personal information was not secured), Defendant had an obligation to disclose the data breach

in a timely and accurate fashion as mandated by Wash. Rev. Code Ann. § 19.255.010(1). However, Defendant breached that obligation.

165. As a direct and proximate result of Defendant's violations of Wash. Rev. Code Ann. § 19.255.010(1), Plaintiff and Washington Sub-Class members suffered damages, as described above.

166. Plaintiff and Washington Sub-Class members seek relief under Wash. Rev. Code Ann. § 19.255.040(3)(a) including, but not limited to, actual damages and injunctive relief.

NINTH CLAIM
WASHINGTON UNIFORM HEALTH CARE INFORMATION ACT, WASH. REV. CODE §§ 70.02.020, 70.02.170
(On behalf of the Washington Sub-Class)

167. Plaintiff incorporates and realleges the allegations in the preceding paragraphs as if fully set forth herein.

168. Plaintiff brings this claim against Defendant operating in Washington on behalf of herself and the Washington Sub-Class whose personal information was compromised as a result of the Apria Breaches.

169. Defendant is a "health care provider," as defined in Wash. Rev. Code Ann. §§ 70.02.010(15), 70.02.010(19) because it provides health care in the ordinary course of business and is self-described as "a leading provider of home medical equipment and clinical support."[27] Defendant further states "Apria's Care Team members are able to support our patients' treatment plans and supplement with additional services, if needed."[28]

[27] *About Us*, Apria, https://www.apria.com/about-us (last visited June 14, 2023).
[28] *Id.*

170. As a result of providing healthcare in Washington, Defendant possessed personal information including personal health care information pertaining to Plaintiff and members of the Washington Sub-Class.

171. Defendant released personal information, including health care information, regarding Plaintiff and members of the Washington Sub-Class without authorization in violation of Wash. Rev. Code § 70.02.020.

172. Plaintiff and members of the Washington Sub-Class were injured and have suffered damages from Defendant's illegal disclosure and negligent release of their personal information, including health care information in violation of Wash. Rev. Code § 70.02.020.

173. Plaintiff and members of the Washington Sub-Class seek relief under Wash. Rev. Code § 70.02.170, including but not limited to, actual damages, injunctive relief, and/or attorneys' fees and costs.

VII. PRAYER FOR RELIEF

WHEREFORE, Plaintiff requests that this Court enter a judgment against Defendant and in favor of Plaintiff and the Class and Sub-Class, and award the following relief:

a. that this action be certified as a class action pursuant to Rule 23 of the Federal Rules of Civil Procedure, declaring Plaintiff as the representative of the Class and Sub-Class, and Plaintiff's counsel as counsel for the Class and Sub-Class;

b. award Plaintiff and members of the Classes appropriate relief, including actual damages, statutory damages, treble damages, punitive damages, and restitutionary disgorgement;

c. award equitable and declaratory relief as may be appropriate, including without limitation meaningful extended credit monitoring services and identity theft protection for Plaintiff and members of the Classes;

d. award all costs of prosecuting the litigation, including expert fees;

e. award pre- and post-judgment interest;

f. award attorneys' fees; and

g. grant such additional relief as this Court may deem just and proper.

VIII. DEMAND FOR JURY TRIAL

Pursuant to Federal Rule of Civil Procedure 38(b), Plaintiff hereby demands a trial by jury.

Dated: June 15, 2023

Respectfully submitted,

/s/ William N. Riley

William N. Riley (#14941-49)
Russell B. Cate (#27056-29)
Sundeep Singh (#26591-29)
RILEYCATE, LLC
11 Municipal Dr., Suite 320
Fishers, IN 46038
Tel: (317) 588-2866
Fax: (317) 458-1785
wriley@rileycate.com
rcate@rileycate.com
ssingh@rileycate.com

Joseph H. Meltzer
Melissa L. Yeates
Jordan E. Jacobson
Varun Elangovan
KESSLER TOPAZ MELTZER & CHECK, LLP
280 King of Prussia Road
Radnor, PA 19087
Tel: (610) 667-7706
Fax: (610 667-7056
jmeltzer@ktmc.com
myeates@ktmc.com
jjacobson@ktmc.com
velangovan@ktmc.com

Attorneys for Plaintiff

JS 44 (Rev. 10/20)

CIVIL COVER SHEET

The JS 44 civil cover sheet and the information contained herein neither replace nor supplement the filing and service of pleadings or other papers as required by law, except as provided by local rules of court. This form, approved by the Judicial Conference of the United States in September 1974, is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. *(SEE INSTRUCTIONS ON NEXT PAGE OF THIS FORM.)*

I. (a) PLAINTIFFS

Suzanne Cuyle, Individually and on Behalf of All Others Similarly Situated

(b) County of Residence of First Listed Plaintiff Snohomish
(EXCEPT IN U.S. PLAINTIFF CASES)

(c) Attorneys *(Firm Name, Address, and Telephone Number)*
RileyCate, LLC, 11 Municipal Dr., Suite 320, Fishers, IN 46038 Tel: (317) 588-2866

DEFENDANTS

Apria Healthcare, LLC

County of Residence of First Listed Defendant Marion
(IN U.S. PLAINTIFF CASES ONLY)

NOTE: IN LAND CONDEMNATION CASES, USE THE LOCATION OF THE TRACT OF LAND INVOLVED.

Attorneys *(If Known)*

II. BASIS OF JURISDICTION *(Place an "X" in One Box Only)*

- ☐ 1 U.S. Government Plaintiff
- ☐ 3 Federal Question *(U.S. Government Not a Party)*
- ☐ 2 U.S. Government Defendant
- ☒ 4 Diversity *(Indicate Citizenship of Parties in Item III)*

III. CITIZENSHIP OF PRINCIPAL PARTIES *(Place an "X" in One Box for Plaintiff and One Box for Defendant)*
(For Diversity Cases Only)

	PTF	DEF		PTF	DEF
Citizen of This State	☐ 1	☐ 1	Incorporated *or* Principal Place of Business In This State	☐ 4	☒ 4
Citizen of Another State	☒ 2	☐ 2	Incorporated *and* Principal Place of Business In Another State	☐ 5	☐ 5
Citizen or Subject of a Foreign Country	☐ 3	☐ 3	Foreign Nation	☐ 6	☐ 6

IV. NATURE OF SUIT *(Place an "X" in One Box Only)*

Click here for: Nature of Suit Code Descriptions.

CONTRACT
- ☐ 110 Insurance
- ☐ 120 Marine
- ☐ 130 Miller Act
- ☐ 140 Negotiable Instrument
- ☐ 150 Recovery of Overpayment & Enforcement of Judgment
- ☐ 151 Medicare Act
- ☐ 152 Recovery of Defaulted Student Loans (Excludes Veterans)
- ☐ 153 Recovery of Overpayment of Veteran's Benefits
- ☐ 160 Stockholders' Suits
- ☐ 190 Other Contract
- ☐ 195 Contract Product Liability
- ☐ 196 Franchise

REAL PROPERTY
- ☐ 210 Land Condemnation
- ☐ 220 Foreclosure
- ☐ 230 Rent Lease & Ejectment
- ☐ 240 Torts to Land
- ☐ 245 Tort Product Liability
- ☐ 290 All Other Real Property

TORTS

PERSONAL INJURY
- ☐ 310 Airplane
- ☐ 315 Airplane Product Liability
- ☐ 320 Assault, Libel & Slander
- ☐ 330 Federal Employers' Liability
- ☐ 340 Marine
- ☐ 345 Marine Product Liability
- ☐ 350 Motor Vehicle
- ☐ 355 Motor Vehicle Product Liability
- ☐ 360 Other Personal Injury
- ☐ 362 Personal Injury - Medical Malpractice

PERSONAL INJURY
- ☐ 365 Personal Injury - Product Liability
- ☐ 367 Health Care/ Pharmaceutical Personal Injury Product Liability
- ☐ 368 Asbestos Personal Injury Product Liability

PERSONAL PROPERTY
- ☒ 370 Other Fraud
- ☐ 371 Truth in Lending
- ☐ 380 Other Personal Property Damage
- ☐ 385 Property Damage Product Liability

CIVIL RIGHTS
- ☐ 440 Other Civil Rights
- ☐ 441 Voting
- ☐ 442 Employment
- ☐ 443 Housing/ Accommodations
- ☐ 445 Amer. w/Disabilities - Employment
- ☐ 446 Amer. w/Disabilities - Other
- ☐ 448 Education

PRISONER PETITIONS

Habeas Corpus:
- ☐ 463 Alien Detainee
- ☐ 510 Motions to Vacate Sentence
- ☐ 530 General
- ☐ 535 Death Penalty

Other:
- ☐ 540 Mandamus & Other
- ☐ 550 Civil Rights
- ☐ 555 Prison Condition
- ☐ 560 Civil Detainee - Conditions of Confinement

FORFEITURE/PENALTY
- ☐ 625 Drug Related Seizure of Property 21 USC 881
- ☐ 690 Other

LABOR
- ☐ 710 Fair Labor Standards Act
- ☐ 720 Labor/Management Relations
- ☐ 740 Railway Labor Act
- ☐ 751 Family and Medical Leave Act
- ☐ 790 Other Labor Litigation
- ☐ 791 Employee Retirement Income Security Act

IMMIGRATION
- ☐ 462 Naturalization Application
- ☐ 465 Other Immigration Actions

BANKRUPTCY
- ☐ 422 Appeal 28 USC 158
- ☐ 423 Withdrawal 28 USC 157

PROPERTY RIGHTS
- ☐ 820 Copyrights
- ☐ 830 Patent
- ☐ 835 Patent - Abbreviated New Drug Application
- ☐ 840 Trademark
- ☐ 880 Defend Trade Secrets Act of 2016

SOCIAL SECURITY
- ☐ 861 HIA (1395ff)
- ☐ 862 Black Lung (923)
- ☐ 863 DIWC/DIWW (405(g))
- ☐ 864 SSID Title XVI
- ☐ 865 RSI (405(g))

FEDERAL TAX SUITS
- ☐ 870 Taxes (U.S. Plaintiff or Defendant)
- ☐ 871 IRS—Third Party 26 USC 7609

OTHER STATUTES
- ☐ 375 False Claims Act
- ☐ 376 Qui Tam (31 USC 3729(a))
- ☐ 400 State Reapportionment
- ☐ 410 Antitrust
- ☐ 430 Banks and Banking
- ☐ 450 Commerce
- ☐ 460 Deportation
- ☐ 470 Racketeer Influenced and Corrupt Organizations
- ☐ 480 Consumer Credit (15 USC 1681 or 1692)
- ☐ 485 Telephone Consumer Protection Act
- ☐ 490 Cable/Sat TV
- ☐ 850 Securities/Commodities/ Exchange
- ☐ 890 Other Statutory Actions
- ☐ 891 Agricultural Acts
- ☐ 893 Environmental Matters
- ☐ 895 Freedom of Information Act
- ☐ 896 Arbitration
- ☐ 899 Administrative Procedure Act/Review or Appeal of Agency Decision
- ☐ 950 Constitutionality of State Statutes

V. ORIGIN *(Place an "X" in One Box Only)*

☒ 1 Original Proceeding | ☐ 2 Removed from State Court | ☐ 3 Remanded from Appellate Court | ☐ 4 Reinstated or Reopened | ☐ 5 Transferred from Another District *(specify)* | ☐ 6 Multidistrict Litigation - Transfer | ☐ 8 Multidistrict Litigation - Direct File

VI. CAUSE OF ACTION

Cite the U.S. Civil Statute under which you are filing ***(Do not cite jurisdictional statutes unless diversity)***:
28 U.S.C. § 1332(d)(2)

Brief description of cause:
Data Breach Action

VII. REQUESTED IN COMPLAINT:

☒ CHECK IF THIS IS A **CLASS ACTION** UNDER RULE 23, F.R.Cv.P.

DEMAND $

CHECK YES only if demanded in complaint:
JURY DEMAND: ☒ Yes ☐ No

VIII. RELATED CASE(S) IF ANY

(See instructions): JUDGE _____ DOCKET NUMBER _____

DATE: June 15, 2023

SIGNATURE OF ATTORNEY OF RECORD: /s/ William N. Riley

FOR OFFICE USE ONLY

RECEIPT # _____ AMOUNT _____ APPLYING IFP _____ JUDGE _____ MAG. JUDGE _____

INSTRUCTIONS FOR ATTORNEYS COMPLETING CIVIL COVER SHEET FORM JS 44

Authority For Civil Cover Sheet

The JS 44 civil cover sheet and the information contained herein neither replaces nor supplements the filings and service of pleading or other papers as required by law, except as provided by local rules of court. This form, approved by the Judicial Conference of the United States in September 1974, is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. Consequently, a civil cover sheet is submitted to the Clerk of Court for each civil complaint filed. The attorney filing a case should complete the form as follows:

I.(a) **Plaintiffs-Defendants.** Enter names (last, first, middle initial) of plaintiff and defendant. If the plaintiff or defendant is a government agency, use only the full name or standard abbreviations. If the plaintiff or defendant is an official within a government agency, identify first the agency and then the official, giving both name and title.

(b) **County of Residence.** For each civil case filed, except U.S. plaintiff cases, enter the name of the county where the first listed plaintiff resides at the time of filing. In U.S. plaintiff cases, enter the name of the county in which the first listed defendant resides at the time of filing. (NOTE: In land condemnation cases, the county of residence of the "defendant" is the location of the tract of land involved.)

(c) **Attorneys.** Enter the firm name, address, telephone number, and attorney of record. If there are several attorneys, list them on an attachment, noting in this section "(see attachment)".

II. **Jurisdiction.** The basis of jurisdiction is set forth under Rule 8(a), F.R.Cv.P., which requires that jurisdictions be shown in pleadings. Place an "X" in one of the boxes. If there is more than one basis of jurisdiction, precedence is given in the order shown below.
United States plaintiff. (1) Jurisdiction based on 28 U.S.C. 1345 and 1348. Suits by agencies and officers of the United States are included here.
United States defendant. (2) When the plaintiff is suing the United States, its officers or agencies, place an "X" in this box.
Federal question. (3) This refers to suits under 28 U.S.C. 1331, where jurisdiction arises under the Constitution of the United States, an amendment to the Constitution, an act of Congress or a treaty of the United States. In cases where the U.S. is a party, the U.S. plaintiff or defendant code takes precedence, and box 1 or 2 should be marked.
Diversity of citizenship. (4) This refers to suits under 28 U.S.C. 1332, where parties are citizens of different states. When Box 4 is checked, the citizenship of the different parties must be checked. (See Section III below**; NOTE: federal question actions take precedence over diversity cases.**)

III. **Residence (citizenship) of Principal Parties.** This section of the JS 44 is to be completed if diversity of citizenship was indicated above. Mark this section for each principal party.

IV. **Nature of Suit.** Place an "X" in the appropriate box. If there are multiple nature of suit codes associated with the case, pick the nature of suit code that is most applicable. Click here for: Nature of Suit Code Descriptions.

V. **Origin.** Place an "X" in one of the seven boxes.
Original Proceedings. (1) Cases which originate in the United States district courts.
Removed from State Court. (2) Proceedings initiated in state courts may be removed to the district courts under Title 28 U.S.C., Section 1441.
Remanded from Appellate Court. (3) Check this box for cases remanded to the district court for further action. Use the date of remand as the filing date.
Reinstated or Reopened. (4) Check this box for cases reinstated or reopened in the district court. Use the reopening date as the filing date.
Transferred from Another District. (5) For cases transferred under Title 28 U.S.C. Section 1404(a). Do not use this for within district transfers or multidistrict litigation transfers.
Multidistrict Litigation – Transfer. (6) Check this box when a multidistrict case is transferred into the district under authority of Title 28 U.S.C. Section 1407.
Multidistrict Litigation – Direct File. (8) Check this box when a multidistrict case is filed in the same district as the Master MDL docket.
PLEASE NOTE THAT THERE IS NOT AN ORIGIN CODE 7. Origin Code 7 was used for historical records and is no longer relevant due to changes in statue.

VI. **Cause of Action.** Report the civil statute directly related to the cause of action and give a brief description of the cause. **Do not cite jurisdictional statutes unless diversity.** Example: U.S. Civil Statute: 47 USC 553 Brief Description: Unauthorized reception of cable service.

VII. **Requested in Complaint.** Class Action. Place an "X" in this box if you are filing a class action under Rule 23, F.R.Cv.P.
Demand. In this space enter the actual dollar amount being demanded or indicate other demand, such as a preliminary injunction.
Jury Demand. Check the appropriate box to indicate whether or not a jury is being demanded.

VIII. **Related Cases.** This section of the JS 44 is used to reference related pending cases, if any. If there are related pending cases, insert the docket numbers and the corresponding judge names for such cases.

Date and Attorney Signature. Date and sign the civil cover sheet.

AO 440 (Rev. 06/12) Summons in a Civil Action

UNITED STATES DISTRICT COURT

for the

Southern District of Indiana

SUZANNE CUYLE, Individually and on Behalf of Alll Others Similarly Situated,

Plaintiff(s)

v.

APRIA HEALTHCARE, LLC

Defendant(s)

Civil Action No. 1:23-cv-1042

SUMMONS IN A CIVIL ACTION

To: *(Defendant's name and address)* Apria Healthcare, LLC
c/o National Registered Agents, Inc.
334 North Senate Avenue
Indianapolis, IN 46204

A lawsuit has been filed against you.

Within 21 days after service of this summons on you (not counting the day you received it) — or 60 days if you are the United States or a United States agency, or an officer or employee of the United States described in Fed. R. Civ. P. 12 (a)(2) or (3) — you must serve on the plaintiff an answer to the attached complaint or a motion under Rule 12 of the Federal Rules of Civil Procedure. The answer or motion must be served on the plaintiff or plaintiff's attorney, whose name and address are: William N. Riley
RileyCate, LLC
11 Municipal Dr., Suite 320
Fishers, IN 46038

If you fail to respond, judgment by default will be entered against you for the relief demanded in the complaint. You also must file your answer or motion with the court.

CLERK OF COURT

Date: _____

_____
Signature of Clerk or Deputy Clerk

Civil Action No.

PROOF OF SERVICE

(This section should not be filed with the court unless required by Fed. R. Civ. P. 4 (l))

This summons for *(name of individual and title, if any)* _____ was received by me on *(date)* _____ .

❒ I personally served the summons on the individual at *(place)* _____ on *(date)* _____ ; or

❒ I left the summons at the individual's residence or usual place of abode with *(name)* _____ , a person of suitable age and discretion who resides there, on *(date)* _____ , and mailed a copy to the individual's last known address; or

❒ I served the summons on *(name of individual)* _____ , who is designated by law to accept service of process on behalf of *(name of organization)* _____ on *(date)* _____ ; or

❒ I returned the summons unexecuted because _____ ; or

❒ Other *(specify):*

My fees are $ _____ for travel and $ _____ for services, for a total of $ 0.00 .

I declare under penalty of perjury that this information is true.

Date: _____

_____
Server's signature

_____
Printed name and title

_____
Server's address

Additional information regarding attempted service, etc:

Erin Amos

From: do_not_reply@psc.uscourts.gov
Sent: Thursday, June 15, 2023 3:30 PM
To: Erin Amos
Subject: Pay.gov Payment Confirmation: INDIANA SOUTHERN DISTRICT COURT

Your payment has been successfully processed and the details are below. If you have any questions or you wish to cancel this payment, please contact: INSD Finance Office at 317-229-3912.

Account Number: 6247295
Court: INDIANA SOUTHERN DISTRICT COURT
Amount: $402.00
Tracking Id: AINSDC-7678899
Approval Code: 09520E
Card Number: **********7282
Date/Time: 06/15/2023 03:30:16 ET

NOTE: This is an automated message. Please do not reply