EXHIBIT A(6)

UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF INDIANA
INDIANAPOLIS DIVISION

CHAD HOHENBERY, on behalf of himself and all others similarly situated, Plaintiff, v. APRIA HEALTHCARE LLC, Defendant.	Case No._____ **CLASS ACTION COMPLAINT** JURY TRIAL DEMAND

Plaintiff Chad Hohenbery, on behalf of himself and all other individuals similarly situated, allege the following against Apria Healthcare LLC and bring this Class Action Complaint ("Apria" or "Defendant") based upon personal knowledge with respect to himself and on information and belief derived from, among other things, investigation of counsel and review of public documents as to all other matters:

I. INTRODUCTION

1. Plaintiff brings this class action against Apria Healthcare LLC for its failure to properly secure and safeguard Plaintiff's and other similarly situated Apria patients' and customers' sensitive private information.

2. Apria Healthcare LLC provides a variety of products and services to patients throughout the country. Apria primarily provides equipment for use at home in treating sleep apnea, but also provides pharmaceutical services and equipment for the treatment of other

conditions, such as diabetes. Apria employes roughly 6,500 people and serves millions of patients year to year.[1]

3. In 2019, Defendant Apria experienced a cyberattack, when from April 5, 2019, to May 7, 2019, third parties gained access to Apria's network and were able to view and acquire sensitive personal information stored therein belonging to Apria's patients and customers. In 2021, Defendant experienced *another* cyberattack, where from August 27, 2021, through October 10, 2021, third parties were once again able to access and acquire information stored on Defendant's network (both incidents together, the "Data Breaches").

4. Several years later, in May 2023, Defendant began sending letters to individuals whose information was compromised in the Data Breaches. In these letters, Defendant acknowledged the importance of data security and admitted that it had allowed third parties to gain unauthorized access to its network. It further clarified that the information compromised in the Data Breaches may have included Plaintiff's and Class Members' personal identifying information ("PII") such as their names, addresses, phone numbers, email addresses, dates of birth, drivers' license numbers and/or state identification numbers, and Social Security numbers. The Data Breaches may further have compromised Plaintiff's and Class Members' personal health information ("PHI") including diagnosis and treatment information, health insurance information, and medical billing information (PII together with PHI referred to herein as "Private Information").

5. The Data Breaches occurred because of Defendant's failure to implement reasonable cybersecurity practices and policies. Although Defendant understands its legal obligations to protect Plaintiff's and Class Members' Private Information, Defendant failed to put in place procedures to protect all of the Private Information it collected in the course of its business.

[1] www.apria.com (last accessed on June 19, 2023)

6. As a result, Plaintiff and Class Members are exposed to an ongoing and lifetime risk of identity theft and fraud, which is further heightened by the exposure of Social Security numbers and PHI.

7. Plaintiff and Class Members have suffered injury because of Apria's conduct. The injuries suffered by Plaintiff and Class Members as a direct result of the Data Breaches include, *inter alia*: (i) fraudulent misuse of the stolen Private Information that is traceable to the Data Breaches; (ii) lost or diminished value of Private Information; (iii) out-of-pocket costs and expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their Private Information; (iv) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breaches, including by limited to lost time; and (v) the present and immediate risk to their Private Information, which remains, upon information and belief, unsecured and available for unauthorized third parties to access and abuse, and which remains backed up in Defendant's possession and is therefore subject to further disclosures so long as Defendant fails to implement reasonable security practices and procedures to protect Plaintiff's and Class Members' Private Information.

8. Plaintiff brings this action on behalf of all persons whose Private Information was compromised due to Apria's failure to: (i) adequately protect its patients Private Information, (ii) warn users of its inadequate information security practices, and (iii) effectively monitor its network and platforms for security vulnerabilities and incidents. Apria's conduct amounts to negligence and violates federal and state statutes.

II. JURISDICTION AND VENUE

9. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million exclusive of interest and costs. At least one member of the class is a citizen of a state different from Apria.

10. This Court has personal jurisdiction over Apria because it is a limited liability company organized under the laws of the State of Indiana, because it regularly conducts business in Indiana, has sufficient minimum contacts in Indiana, including its principal place of business, and intentionally avails itself of this jurisdiction by marketing and selling products and services in Indiana.

11. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(a)(1) because a substantial part of the events and omissions giving rise to this action occurred in this District, including (upon information and belief) the data security incident involving Apria's website. Defendant caused harm to Plaintiff and the Class Members through its actions in this District.

III. PARTIES

12. Plaintiff Chad Hohenbery is a citizen of Illinois residing in Bartonville, Illinois in Peoria County. On or about June 6, 2023, Plaintiff Hohenbery received a Data Breach Notice Letter from Defendant informing him of his exposure in the Data Breaches.

13. Defendant Apria, LLC is a foreign limited liability company organized under the laws of the State of Delaware, with a principal place of business at 7353 Company Drive, Indianapolis, IN 46237-9274. As of June 19, 2023, Defendant has one member of its LLC, which, upon information and belief, is Apria Healthcare Group LLC. Apria Healthcare Group LLC is a foreign limited liability company organized under the laws of the State of Delaware, with a principal place of business at 7353 Company Drive, Indianapolis, IN 46237. The sole member of

Apria Healthcare Group LLC is Apria Holdco LLC, which is also a foreign limited liability company organized under the laws of the State of Delaware.

IV. FACTUAL ALLEGATIONS

Background

14. Apria is a company that provides home medical equipment for sleep apnea care, as well as pharmaceutical services and equipment and supplies for diabetes and general wound care. Defendant services millions of customers across the country.[2]

15. In the course of its business as a medical services and equipment provider, Defendant collects sensitive personal information, including PII and PHI from its patients and customers. Plaintiff and Class Members are, or were, among those patients and customers and relied upon the sophistication, resources, and assurances of Defendant to keep their Private Information confidential and secure. Plaintiff and Class Members relied on Defendant to use this Private Information only for authorized purposes and only to make authorized disclosures of this information.

16. Defendant had a duty to adopt reasonable measures to protect Plaintiff's and Class Members' Private Information from involuntary and/or unauthorized disclosures to third parties.

The Data Breaches

17. Defendant Apria Healthcare LLC experienced a Data Breach between April 5, 2019, and May 7, 2019, and a separate Data Breach between August 27, 2021, and October 10, 2021. In each of these Data Breaches, unauthorized third parties were able to infiltrate Defendant's network and gain access to the Private Information of Defendant's patients and customers,

[2] *Id*.

including PII and PHI. These third parties were able to access and acquire information, undetected and undeterred, for several months during 2019 and 2021.

18. It was not until late May 2023 that Defendant began notifying Plaintiff and Class members of the Data Breaches, and the Private Information compromised during these attacks. In some instances, Plaintiff and Class Members were unknowingly placed at substantially heightened risk for identity theft and fraud for more than four years by Defendant.

19. Defendant's inadequate data security policies and procedures placed Plaintiff and Class Members at risk, and as a result, exposed their Private Information in the Data Breaches. From the moment that their Private Information was compromised in the Data Breaches, Plaintiff and Class Members have faced an increased risk of fraud and identity theft, and must live on with that threat indefinitely.

20. Defendant had obligations to protect Plaintiff's and Class Members' Private Information from this kind of unauthorized access and disclosure.

21. Plaintiff and Class Members provided their Private Information to Defendant with the reasonable expectation and mutual understanding that Defendant would comply with their obligations to protect that Private Information and keep it safe, secure, and confidential in compliance with both Defendant's legal and ethical obligations.

22. Defendant knew or should have known that these attacks were common and foreseeable. In 2022, there were 1,802 data breaches, nearly eclipsing 2021's record wherein 1,862 data breaches occurred, resulting in approximately 293,927,708 sensitive records being exposed, a 68 percent increase from 2020. [3] The 330 reported breaches reported in 2021 exposed nearly 30

[3] *See* 2021 Data Breach Annual Report (ITRC, Jan. 2022) (available at https://notified.idtheftcenter.org/s/), at 6 (last accessed on June 19, 2023)

million sensitive records (28,045,658), compared to only 306 breaches that exposed nearly 10 million sensitive records (9,700,238) in 2020.[4]

23. Indeed, cyberattacks have become so notorious that the Federal Bureau of Investigation ("FBI") and U.S. Secret Service have issued a warning to potential targets, so they are aware of, and prepared for, a potential attack. As one report explained, "[e]ntities like smaller municipalities . . . are attractive to ransomware criminals . . . because they often have lesser IT defenses and a high incentive to regain access to their data quickly."[5]

24. The increase in such attacks, and the resulting risk of future attacks, was widely known to the public and to anyone in the Defendant's industry, including Defendant.

FTC, NIST Guidelines on Protecting Customer Personal Information

25. The Federal Trade Commission ("FTC") has held that the failure to employ reasonable measures to protect against unauthorized access to confidential consumer data constitutes an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA") (codified by 15 U.S.C. § 45).

26. Under the FTCA, Apria is prohibited from engaging in "unfair or deceptive acts or practices in or affecting commerce." The FTC has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of the FTCA.

---

[4] *See Data Breaches Hit Lots More People in 2022* (Jan. 25, 2023) https://www.cnet.com/tech/services-and-software/data-breaches-hit-lots-more-people-in-2022/ (last accessed on June 19, 2023).

[5] FBI, Secret Service Warn of Targeted, Law360 (Nov. 18, 2019), *available at*: https://www.law360.com/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware (last accessed on June 13, 2023).

27. Beginning in 2007, the FTC released a set of industry standards related to data security and the data security practices of businesses, called "Protecting Personal Information: A Guide for Businesses" (the "FTC Guide").[6] In 2011, this guidance was updated to include fundamental data security principles for businesses. In addition to the necessity to protect consumer data, the guide established that:

- Businesses should dispose of personal identifiable information that is no longer needed;
- Businesses should encrypt personal identifiable information and protected cardholder data stored on computer networks so that it is unreadable even if hackers are able to gain access to the information;
- Businesses should thoroughly understand the types of vulnerabilities on their network (of which malware on a point-of-sale system is one) and how to address said vulnerabilities;
- Businesses should implement protocols necessary to correct security breaches;
- Businesses should install intrusion detection systems to expose security breaches at the moment they occur;
- Businesses should install monitoring mechanisms to watch for massive troves of data being transmitted from their systems; and,
- Businesses should have an emergency plan prepared in response to a breach.

28. On information and belief, Apria failed to adequately address the foregoing requirements in the FTC Guide.

[6] *See FTC Unveils Practice Suggestions for Businesses on Safeguarding Personal Information*, FEDERAL TRADE COMM'N (Mar. 8, 2007), https://www.ftc.gov/news-events/press-releases/2007/03/ftc-unveils-practical-suggestions-businesses-safeguarding; *see also* Fed. Trade Comm'n, *Protecting Personal Information: A Guide for Business, Federal Trade Commission* (Oct. 2016), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal information.pdf (updated FTC Guide).

29. In 2015, the FTC supplemented the FTC Guide with a publication called "Start with Security" (the "**Supplemented FTC Guide**").[7] This supplement added further requirements for businesses that maintain customer data on their networks:

- Businesses should not keep personal identifiable information and protected cardholder data stored on their networks for any period longer than what is needed for authorization;
- Businesses should use industry-tested methods for data security; and,
- Businesses should be continuously monitoring for suspicious activity on their network.

30. Again, Apria failed to adequately address these requirements enumerated in the Supplemented FTC Guide.

31. The FTC Guide is clear that businesses should, among other things: (1) protect the personal customer information they acquire; (2) properly dispose of personal information that is no longer needed; (3) encrypt information stored on computer networks; (4) understand their network's vulnerabilities; and (5) implement policies for installing vendor-approved patches to correct security vulnerabilities. The FTC guidance also recommends that businesses: (1) use an intrusion detection system to expose a breach as soon as it occurs; (2) monitor all incoming traffic for activity indicating that someone may be trying to penetrate the system; and (3) watch for large amounts of data being transmitted from the system.[8] Plaintiff believe that Apria did not follow these recommendations, and as a result exposed hundreds of thousands of consumers to harm.

---

[7] Fed. Trade Comm'n, Start with Security: A Guide for Business (June 2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf

[8] *See, e.g.*, *id.*; Fed. Trade Comm'n, *Protecting Personal Information: A Guide for Business* (Oct. 2016), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.

32. Furthermore, the FTC has issued orders against businesses for failing to employ reasonable measures to safeguard customer data. The orders provide further public guidance to businesses concerning their data security obligations.

33. Apria knew or should have known about its obligation to comply with the FTCA, the FTC Guide, the Supplemented FTC Guide, and many other FTC pronouncements regarding data security.

34. Thus, among other things, Apria's misconduct violated the FTCA and the FTC's data security pronouncements, led to the Data Breach, and resulted directly and proximately in harm to Plaintiff and the Class Members.

35. Additionally, the National Institute of Standards and Technology ("NIST") provides basic network security guidance that enumerates steps to take to avoid cybersecurity vulnerabilities.[9] Although use of NIST guidance is voluntary, the guidelines provide valuable insights and best practices to protect network systems and data.

36. NIST guidance includes recommendations for risk assessments, risk management strategies, system access controls, training, data security, network monitoring, breach detection, and mitigation of existing anomalies.[10]

37. Apria's failure to protect massive amounts of Private Information throughout the multi-month breach periods belies any assertion that Apria employed proper data security protocols or adhered to the spirit of the NIST guidance.

---

[9] *Framework for Improving Critical Infrastructure Cybersecurity*, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (April 16, 2018), Appendix A, Table 2, *available at* https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.

[10] *Id*. at Table 2 pg. 36-43.

Value of Personally Identifiable Information

38. PII is a valuable property right. Its value is axiomatic, considering the value of big data in corporate America and the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that Private Information has considerable market value.

39. The Private Information of consumers remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark-web pricing for stolen identity credentials. For example, Private Information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[11] Experian reports that a stolen credit or debit card number can sell for $5 to $110 on the dark web; the *fullz* sold for $30 in 2017.[12] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[13]

40. A study by the Identity Theft Resource Center shows the multitude of harms caused by fraudulent use of Private Information:[14]

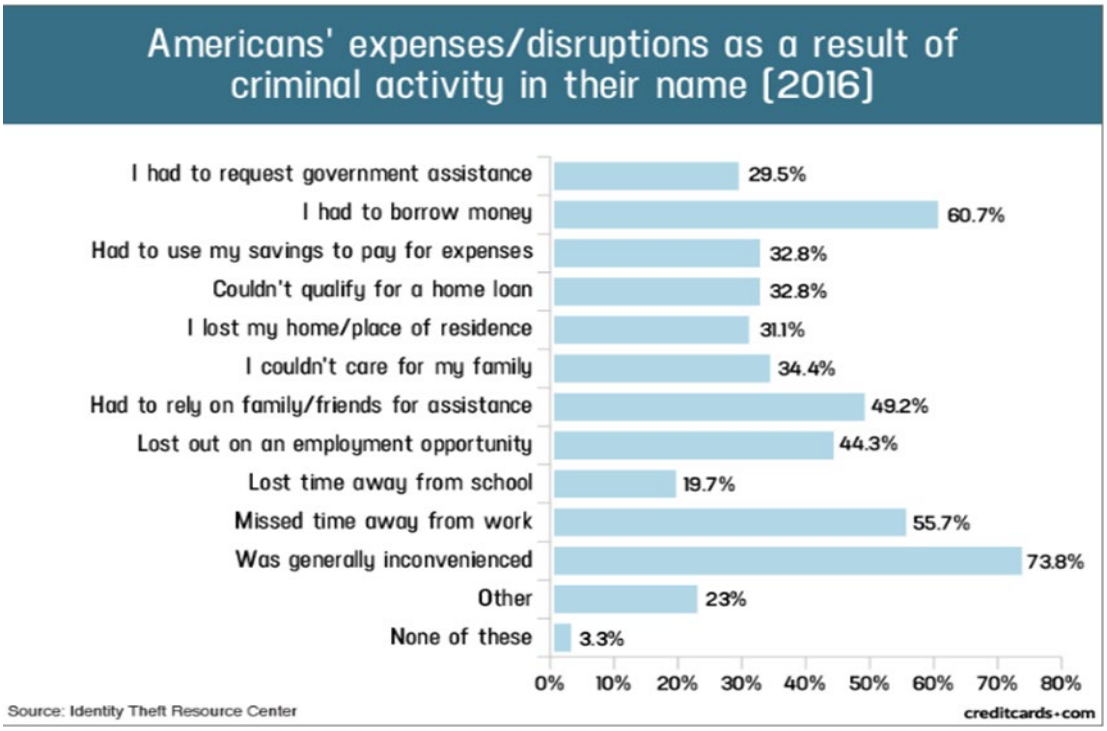
---

[11] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends, Oct. 16, 2019, *available at*: https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/, last accessed May 24, 2021.

[12] *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, *available at*: https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/, last accessed May 24, 2021.

[13] *In the Dark*, VPNOverview, 2019, *available at*: https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/, last accessed May 24, 2021.

[14] Source: "*Credit Card and ID Theft Statistics*" by Jason Steele, 10/24/17, at:https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276/ (last visited October 27, 2020).



41. Plaintiff and the Class Members have experienced one or more of these harms as a result of the Data Breach.

42. Moreover, there may be a time lag between when harm occurs versus when it is discovered, and between when Private Information is stolen and when it is used. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[15]

[15] "Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown" by GAO, June 2007, at: https://www.gao.gov/assets/270/262904.html (last accessed May 24, 2021).

43. Therefore, given the importance of safeguarding Private Information and of the foreseeable consequences that would occur if its data security system was breached, including, specifically, the significant costs that would be imposed on its customers as a result of a breach, Apria was, or should have been, fully aware of its responsibilities towards protecting customer Private Information.

Damage to Plaintiff and the Class Members Caused by the Data Breach

44. Plaintiff and the Class Members have been damaged because their Private Information, including PHI, was accessed by unauthorized third parties in the Data Breaches.

45. Credit monitoring alone is insufficient to remedy the harm to Plaintiff and the Class Members. Plaintiff and the Class Members have or will suffer actual injury as a direct result of Apria's Data Breaches. As a direct and proximate result of Apria's conduct, Plaintiff and the Class have been placed at an imminent, immediate, and continuing increased risk of harm from fraud. Plaintiff and the Class Members now have to take the time and effort to mitigate the actual and potential impact of the data breach on their everyday lives.

46. For example, in addition to fraudulent charges and damage to their credit, many victims have spent and/or will spend substantial time and expense relating to:

a. Finding fraudulent charges;

b. Canceling and reissuing cards;

c. Purchasing identity theft prevention products beyond just credit monitoring;

d. Addressing their inability to withdraw funds linked to compromised accounts;

e. Removing withdrawal and purchase limits on compromised accounts;

f. Taking trips to banks and waiting in line to obtain funds held in limited accounts;

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

h. Resetting automatic billing instructions; and/or

i. Paying late fees and declined payment fees imposed as a result of failed automatic payments.

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

48. Plaintiff and the Class Members also suffered a loss of value of their Private Information when it was acquired by cyber thieves in the Data Breach. Numerous courts have recognized the propriety of loss of value damages in related cases.

49. Plaintiff and the Class Members were also damaged via benefit-of-the-bargain damages. The implied contractual bargain entered into between Apria and Plaintiff and the Class Members included Apria's contractual obligation to provide adequate data security, which Apria failed to provide. Thus, Plaintiff and the Class Members did not get what they paid for, resulting in actual harm.

50. Plaintiff and the Class have suffered, and continue to suffer, economic damages and other actual harm for which they are entitled to compensation, including:

a. Trespass, damage to and theft of their personal property including their Private Information;

b. Improper disclosure of their Private Information property;

c. The imminent and certainly impending injury flowing from potential fraud and identity theft posed by customers' Private Information being placed in the hands of

criminals and having been already misused via the sale of such information on the Internet black market;

d. Damages flowing from Apria's untimely and inadequate notification of the data breach;

e. Loss of privacy suffered as a result of the data breach;

f. Ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the data breach;

g. Ascertainable losses in the form of deprivation of the value of customers' Private Information for which there is a well-established and quantifiable national and international market; and

h. The loss of use of and access to their account funds and costs associated with inability to obtain money from their accounts or being limited in the amount of money customers were permitted to obtain from their accounts.

51. The substantial delay in providing notice of the Data Breach deprived Plaintiff and the Class Members of the ability to promptly mitigate potential adverse consequences resulting from the Data Breach. As a result of Apria's delay in detecting and notifying consumers of the Data Breach, the risk of fraud for Plaintiff and the Class Members was and has been driven even higher.

Plaintiff Chad Hohenbery

52. Plaintiff Chad Hohenbery has been a customer, patient, and employee of Defendant Apria since May 23, 2016.

53. On or about June 6, 2023, Plaintiff Hohenbery received a Data Breach Notice Letter from Defendant informing him that his Private Information may have been compromised in Data

Breaches dating back to 2019. This was the first Plaintiff Hohenbery had heard of either Data Breach.

54. The Data Breach Notice Letter informed Plaintiff Hohenbery that the Private Information of his compromised in the Data Breaches included, but is not limited to, his Social Security Number.

55. Since April 5, 2019, the beginning of the first Data Breach, Plaintiff Hohenbery has experienced unauthorized transactions on his personal financial accounts, prompting him to seek the advice of legal counsel.

56. Plaintiff Hohenbery suffered actual injury in the form of lost time spent dealing with the consequences of the Data Breaches and/or attempting to mitigate further harm.

57. Plaintiff Hohenbery would not have used her Defendant Apria's services had Apria disclosed that it lacked adequate computer systems and data security practices to safeguard customers' Private Information from theft, and that it would not notify its patients and customers of its data vulnerabilities and breaches until they have been exposed for several years.

58. Plaintiff Hohenbery suffered actual injury from having his Private Information compromised and/or stolen as a result of the Data Breaches.

59. Plaintiff Hohenbery suffered actual injury and damages in paying money to and purchasing products from Apria during the Data Breaches that he would not have paid or purchased had Apria disclosed that it lacked computer systems and data security practices adequate to safeguard customers' personal and financial information and had Apria provided timely and accurate notice of the Data Breaches.

60. Plaintiff Hohenbery suffered actual injury in the form of damages to and diminution in the value of his Private Information—a form of intangible property that the Plaintiff Hohenbery

entrusted to Apria for the purpose of receiving medical care and which was compromised in, and as a result of, the Data Breaches.

61. Plaintiff Hohenbery suffered imminent and impending injury arising from the substantially increased risk of future fraud, identity theft and misuse posed by his personal and healthcare information being placed in the hands of criminals who have already misused such information stolen in the Data Breaches via the sale of Plaintiff Hohenbery's and the Class Members' personal and healthcare information on the Internet black market.

62. Plaintiff Hohenbery has a continuing interest in ensuring that his Private Information, which remains in the possession of Apria, is protected and safeguarded from future breaches.

63. Additionally, Plaintiff Hohenbery has always taken reasonable precautions to protect his Private Information.

V. CLASS ALLEGATIONS

64. Plaintiff brings this action pursuant to Rule 23 of the Federal Rules of Civil Procedure on behalf of himself and on behalf of all other persons similarly situated ("the Class").

65. Plaintiff proposes the following Class definitions, subject to amendment as appropriate:

> **Nationwide Class**:
> All individuals in the United States whose Private Information was compromised as a result of the Data Breaches.
>
> **Illinois Subclass**:
> All residents of Illinois whose Private Information was compromised as a result of the Data Breaches.

66. Excluded from each of the above Classes are Defendant and its parents, members, or subsidiaries, any entities in which it has a controlling interest, as well as its officers, directors,

affiliates, legal representatives, heirs, predecessors, successors, and assigns. Also excluded are any Judge to whom this case is assigned as well as his or her judicial staff and immediate family members.

67. Plaintiff reserves the right to modify or amend the definitions of the proposed Classes before the Court determines whether certification is appropriate.

68. Each of the proposed classes meet the criteria for certification under Fed. R. Civ. P. 23(a), (b)(2), and (b)(3).

69. Numerosity. The Members of the Class are so numerous that joinder of all of them is impracticable. While the exact number of Class Members is unknown to Plaintiff at this time, based on information and belief, the Class consists of thousands of customers of Apria whose data was compromised in the Data Breach.

70. Commonality. There are questions of law and fact common to the Class, which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

a. Whether Apria engaged in the conduct alleged herein;

b. Whether Apria's conduct violated the state consumer protection laws invoked below;

c. When Apria actually learned of the data breach and whether its response was adequate;

d. Whether Apria had a legal duty to adequately protect Plaintiff's and the Class Members' Private Information;

e. Whether Apria breached its legal duty by failing to adequately protect Plaintiff's and the Class Members' Private Information;

f. Whether Apria had a legal duty to provide timely and accurate notice of the data breach to Plaintiff and the Class Members;

g. Whether Apria breached its duty to provide timely and accurate notice of the data breach to Plaintiff and the Class Members;

h. Whether Apria implemented and maintained reasonable security procedures and practices appropriate to the nature of storing Plaintiff's and the Class Members' Private Information;

i. Whether Apria knew or should have known that it did not employ reasonable measures to keep Plaintiff's and the Class Members' Private Information secure and prevent loss or misuse of that Private Information;

j. Whether Apria adequately addressed and fixed the vulnerabilities which permitted the data breach to occur;

k. Whether Plaintiff and the Class Members are entitled to recover actual damages and/or statutory damages;

l. Whether Plaintiff and the other Class Members are entitled to additional credit or identity monitoring beyond what the company is offering and are entitled to other monetary relief; and

m. Whether Plaintiff and the Class Members are entitled to equitable relief, including injunctive relief, restitution, disgorgement, and/or the establishment of a constructive trust.

71. Typicality. Plaintiff's claims are typical of those of other Class Members because Plaintiff's Private Information, like that of every other Class Member, was compromised in the Data Breaches.

72. Adequacy of Representation. Plaintiff will fairly and adequately represent and protect the interests of the Members of the Class. Plaintiff's Counsel are competent and experienced in litigating class actions, including data breach class actions.

73. Predominance. Apria has engaged in a common course of conduct toward Plaintiff and the Class Members, in that all the Plaintiff's and the Class Members' Private Information was stored on the same computer systems and unlawfully accessed in the same way. The common issues arising from Apria's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

74. Superiority. A class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Apria. In contrast, the conduct of this action as a class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class Member.

75. Class certification also is appropriate under Fed. R. Civ. P. 23(b)(2). Apria has acted or has refused to act on grounds generally applicable to the Class, so that final injunctive relief or corresponding declaratory relief is appropriate as to the Class as a whole.

76. Finally, all members of the purposed Classes are readily ascertainable. Apria has access to addresses and other contact information for millions of members of the Classes, which can be used to identify Class Members.

COUNT I
NEGLIGENCE
(On behalf of Plaintiff and the Nationwide Class)

77. Plaintiff incorporates by reference all previous allegations in paragraphs 1-76 as though fully set forth herein.

78. Apria solicited and gathered Private Information, including PHI, of Plaintiff and Class Members, in the course of its business practices.

79. Apria knew, or should have known, of the risks inherent in collecting the Private Information of Plaintiff and the Class Members and the importance of adequate security. On information and belief, Apria had notice that hackers routinely attempted to access and acquire Private Information, and PHI in particular, without authorization. Apria also knew or should have known about numerous, well-publicized data breaches involving other national healthcare related companies.

80. Apria owed duties of care to Plaintiff and the Class Members whose Private Information was entrusted to it. Apria's duties included the following:

a. To exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting and protecting Private Information in its possession;

b. To protect customers' Private Information using reasonable and adequate security procedures and systems that are compliant with the industry standards;

c. To implement processes to quickly detect a data breach and to timely act on warnings about data breaches, and

d. To promptly notify Plaintiff and Class Members of any data breaches.

81. By collecting this data, and using it for commercial gain, Apria had a duty of care to use reasonable means to secure and safeguard its computer property, to prevent disclosure of the Private Information, and to safeguard the Private Information from theft. Apria's duties included a responsibility to implement processes by which it could detect a breach of its security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a data breach.

82. Because Apria knew that a breach of its systems would damage thousands of its customers, including Plaintiff and Class Members, it had a duty to adequately protect their Private Information.

83. Apria owed a duty of care not to subject Plaintiff and Class Members to an unreasonable risk of harm because they were foreseeable and probable victims of any inadequate security practices.

84. Apria knew, or should have known, that its computer systems did not adequately safeguard the Private Information of Plaintiff and Class Members.

85. Apria breached its duties of care by failing to provide, or by acting with reckless disregard for, fair, reasonable, or adequate computer systems and data security practices to safeguard the Private Information of Plaintiff and Class Members.

86. Apria breached its duties of care by failing to promptly identify the Data Breaches and then provide prompt notice of the Data Breaches to the persons whose Private Information was compromised.

87. Apria acted with reckless disregard for the rights of Plaintiff and Class Members by failing to provide prompt and adequate individual notice of the Data Breaches so that they could take measures to protect himself from damages caused by the fraudulent use the Private Information compromised in the data breach.

88. Apria had a special relationship with Plaintiff and Class Members. Plaintiff's and Class Members' willingness to entrust Apria with their Private Information was predicated on the understanding that Apria would take adequate security precautions. Moreover, only Apria had the ability to protect its systems (and the Private Information that it stored on them) from attack.

89. Apria's own conduct also created a foreseeable risk of harm to Plaintiff and Class Members and their Private Information. Apria's misconduct included failing to:

a. Secure access to its servers;

b. Comply with industry standard security practices;

c. Employ adequate network segmentation;

d. Implement adequate system and event monitoring;

e. Install updates and patches in a timely manner; and

f. Implement the systems, policies, and procedures necessary to prevent these types of data breaches.

90. Apria also had independent duties under state laws that required it to reasonably safeguard Plaintiff's and Class Members' Private Information and promptly notify them about the Data Breaches.

91. Apria breached the duties it owed to Plaintiff and Class Members in numerous ways, including:

a. By creating a foreseeable risk of harm through the misconduct previously described;

b. By failing to implement adequate security systems, protocols and practices sufficient to protect Private Information both before and after learning of the data breach;

c. By failing to comply with the minimum industry data security standards during the periods of the data breaches; and

d. By failing to timely and accurately disclose to each class member that the personal information of Plaintiff and the Class had been improperly acquired or accessed.

92. But for Apria's wrongful and negligent breach of the duties it owed Plaintiff and Class Members, their Private Information either would not have been compromised or they would have been able to prevent some or all of their damages.

93. As a direct and proximate result of Apria's negligent conduct, Plaintiff and Class Members have suffered damages and are at imminent risk of further harm.

94. The injury and harm that Plaintiff and Class Members suffered (as alleged above) were reasonably foreseeable.

95. The injury and harm that Plaintiff and Class Members suffered (as alleged above) were the direct and proximate result of Apria's negligent conduct.

96. Plaintiff and Class Members have suffered injury and are entitled to damages in an amount to be proven at trial.

///

///

///

COUNT II
NEGLIGENCE *PER SE*
(On behalf of Plaintiff and the Nationwide Class)

97. Plaintiff incorporates by reference all previous allegations in paragraphs 1-76 as though fully set forth herein.

98. Pursuant to Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45, Apria had a duty to provide fair and adequate computer systems and data security to safeguard the Private Information, including PHI, of Plaintiff and Class Members.

99. The FTCA prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Apria, of failing to use reasonable measures to protect Private Information. The FTC publications and orders described above also form part of the basis of Apria's duty in this regard.

100. Apria solicited, gathered, and stored Private Information, of Plaintiff and the Nationwide Class Members to facilitate sales transactions that affect commerce.

101. Apria violated the FTCA by failing to use reasonable measures to protect Private Information of Plaintiff and the Class and not complying with applicable industry standards, as described herein.

102. Apria's violation of the FTCA constitutes negligence *per se*.

103. Plaintiff and the Nationwide Class Members are within the class of persons that the FTCA was intended to protect.

104. The harm that occurred as a result of the Data Breach is the type of harm the FTCA was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and

deceptive practices, caused the same harm as that suffered by Plaintiff and the Nationwide Class Members.

105. As a direct and proximate result of Apria's negligence *per se*, Plaintiff and the Nationwide Class Members have suffered, and continue to suffer, injuries damages arising from false or fraudulent charges stemming from the data breach, including but not limited to late fees charges; damages from lost time and effort to mitigate the actual and potential impact of the data breach on their lives including, *inter alia*, by contacting their financial institutions to place to dispute fraudulent charges, closing or modifying financial accounts, closely reviewing and monitoring their accounts for unauthorized activity.

106. Apria breached its duties to Plaintiff and the Nationwide Class Members under these laws by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and the Nationwide Class Members' Private Information.

107. But for Apria's wrongful and negligent breach of its duties owed to Plaintiff and the Nationwide Class Members, Plaintiff and the Nationwide Class Members would not have been injured.

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

109. As a direct and proximate result of Apria's negligent conduct, Plaintiff and the Nationwide Class Members have suffered injury and are entitled to compensatory and consequential damages in an amount to be proven at trial.

COUNT III
BREACH OF IMPLIED CONTRACT
(On behalf of Plaintiff and the Nationwide Class)

110. Plaintiff incorporates by reference all previous allegations in paragraphs 1-76 as though fully set forth herein.

111. When Plaintiff and the Nationwide Class Members provided their Private Information to Apria in making purchases on its website, they entered into implied contracts by which Apria agreed to protect their Private Information and timely notify them in the event of a data breach.

112. Apria solicited and invited its customers, including Plaintiff and the Nationwide Class Members, to provide their Private Information and received home medical equipment or medical care services from Defendant in the course of a business transaction.

113. An implicit part of the offer was that Apria would safeguard the Private Information using reasonable or industry-standard means and would timely notify Plaintiff and the Nationwide Class Members in the event of a data breach.

114. Apria also affirmatively represented in its Privacy Policy that it protected the Private Information of Plaintiff and the Nationwide Class Members in several ways, as described above.

115. Based on the implicit understanding and also on Apria's representations, Plaintiff and the Nationwide Class Members accepted the offers and provided Apria with their Private Information.

116. Apria manifested its intent to enter into an implied contract that included a contractual obligation to reasonably protect Plaintiff's and the Nationwide Class Members' Private Information through, among other things, its Privacy Policy.

117. In entering into such implied contracts, Plaintiff and the Nationwide Class Members reasonably believed and expected that Apria's data security practices complied with relevant laws and regulations and were consistent with industry standards.

118. Plaintiff and the Nationwide Class Members would not have provided their Private Information to Apria had they known that Apria would not safeguard their Private Information as promised or provide timely notice of a data breaches.

119. Plaintiff and the Nationwide Class Members fully performed their obligations under the implied contracts with Apria.

120. Apria breached the implied contracts by failing to safeguard Plaintiff's and the Nationwide Class Members' Private Information and failing to provide them with timely and accurate notice when their PII was compromised in the data breach.

121. The losses and damages Plaintiff and the Nationwide Class Members sustained (as described above) were the direct and proximate result of Apria's breaches of its implied contracts with them.

122. Plaintiff and the Nationwide Class Members also are entitled to injunctive relief requiring Apria to, *inter alia*, strengthen its data security systems and monitoring procedures, conduct periodic audits of those systems, and provide lifetime credit monitoring and identity theft insurance to Plaintiff and the Nationwide Class Members.

COUNT IV
UNJUST ENRICHMENT
(On behalf of Plaintiff and the Nationwide Class)

123. Plaintiff incorporates by reference all previous allegations in paragraphs 1-76 as though fully set forth herein.

124. This count is plead in the alternative to Count III above.

125. Plaintiff and members of the Nationwide Class conferred a monetary benefit on Apria. Specifically, they made purchases from Apria and provided Apria with their Private Information that they would not have provided if they had known that Apria did not provide adequate protection of their Private Information.

126. Apria knew that Plaintiff and the Nationwide Class Members conferred a benefit on Apria. Apria profited from their purchases and used their Private Information for its own business purposes.

127. The monies for goods that Plaintiff and the Nationwide Class Members paid to Apria were to be used by Apria, in part, to pay for the administrative costs of reasonable data privacy and security practices and procedures.

128. Apria failed to secure the Plaintiff's and the Nationwide Class Members' Private Information, and therefore, it was unjustly enriched by the purchases made by Plaintiff and the Class that they would not have made had they known that Apria did not keep their personal information secure.

129. Plaintiff and the Nationwide Class Members have no adequate remedy at law.

130. Under the circumstances, it would be unjust for Apria to be permitted to retain any of the benefits that Plaintiff and the Nationwide Class Members conferred on it.

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

///

///

COUNT V
DECLARATORY JUDGMENT
(On Behalf of Plaintiff and the Nationwide Class)

132. Plaintiff incorporates by reference all previous allegations in paragraphs 1-76 as though fully set forth herein.

133. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, *et seq.*, this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal and state statutes described in this Complaint.

134. Apria owes duties of care to Plaintiff and the Nationwide Class Members that required it to adequately secure their Private Information.

135. Apria still possesses Private Information regarding Plaintiff and the Nationwide Class Members.

136. Plaintiff alleges that Apria's data security measures remain inadequate. Apria publicly denies these allegations. Furthermore, Plaintiff continue to suffer injury as a result of the compromise of their Private Information and remain at imminent risk that further compromises of their Private Information will occur in the future.

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

a. Apria owes a legal duty to secure consumers' Private Information and to timely notify consumers of a data breach under the common law and Section 5 of the FTCA;

b. Apria existing security measures do not comply with its explicit or implicit contractual obligations and duties of care to provide reasonable security procedures

and practices appropriate to the nature of the information to protect customers' Private Information;

c. Apria continues to breach this legal duty by failing to employ reasonable measures to secure consumers' Private Information;

d. to comply with its explicit or implicit contractual obligations and duties of care, Apria must implement and maintain reasonable security measures, including, but not limited to:

i. Engaging third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Apria's systems on a periodic basis, and ordering Apria to promptly correct any problems or issues detected by such third-party security auditors;

ii. Engaging third-party security auditors and internal personnel to run automated security monitoring;

iii. Auditing, testing, and training its security personnel regarding any new or modified procedures;

iv. Segmenting its user applications by, among other things, creating firewalls and access controls so that if one area is compromised, hackers cannot gain access to other portions of Apria's systems;

v. Conducting regular database scanning and securing checks;

vi. Routinely and continually conducting internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

vii. Purchasing credit monitoring services for Plaintiff and the Nationwide Class Members for a period of ten years; and

viii. Meaningfully educating its users about the threats they face as a result of the loss of their Private Information to third parties, as well as the steps Apria's customers must take to protect himself.

138. This Court also should issue corresponding prospective injunctive relief requiring Apria to employ adequate security protocols consistent with law and industry standards to protect consumers' Private Information.

139. If an injunction is not issued, Plaintiff and the Nationwide Class Members will suffer irreparable injury, and lack an adequate legal remedy, in the event of another data breach at Apria. The risk of another such breach is real, immediate, and substantial. If another breach at Apria occurs, Plaintiff will not have an adequate remedy at law because many of the resulting injuries are not readily quantifiable.

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

141. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach at Apria, thus eliminating the additional injuries that would result to Plaintiff and consumers whose PII would be further compromised.

COUNT VI
VIOLATION OF THE ILLINOIS CONSUMER FRAUD AND DECEPTIVE BUSINESS PRACTICES ACT ("ILLINOIS CFA"), 815 ILL. COMP. STAT. §§ 505/1, *ET SEQ.*

(On behalf of Plaintiff Hohenbery and the Illinois Subclass)

142. Plaintiff incorporates by reference all previous allegations in paragraphs 1-76 as though fully set forth herein.

143. This Count is brought on behalf of Plaintiff Hohenbery and the Illinois Subclass.

144. Plaintiff Hohenbery and the Illinois Subclass are "consumers" as that term is defined in 815 Ill. Comp. Stat. § 505/1(e).

145. Plaintiff Hohenbery, the Illinois Subclass, and Apria are "persons" as that term is defined in 815 Ill. Comp. Stat. § 505/1(c).

146. Apria is engaged in "trade" or "commerce," including provision of services, as those terms are defined under 815 Ill. Comp. Stat. § 505/1(f).

147. Apria engages in the "sale" of "merchandise" (including services) as defined by 815 Ill. Comp. Stat. § 505/1(b) and (d).

148. Apria engaged in deceptive and unfair acts and practices, misrepresentation, and the concealment, suppression, and omission of material facts in connection with the sale and advertisement of "merchandise" (as defined in the Illinois CFA) in violation of the Illinois CFA, including but not limited to the following:

a. failing to maintain sufficient security to keep Plaintiff Hohenbery's and the Illinois Subclass Members' sensitive Private Information from being hacked and stolen;

b. misrepresenting material facts to Plaintiff Hohenbery and the Illinois Subclass Members, in connection with the sale of goods and services, by representing that it would maintain adequate data privacy and security practices and procedures to

safeguard Plaintiff Hohenbery and the Illinois Subclass Members' Private Information from unauthorized disclosure, release, data breaches, and theft;

c. misrepresenting material facts to Plaintiff Hohenbery and the Illinois Subclass Members in connection with sale of goods and services, by representing that Apria did and would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of Plaintiff Hohenbery and the Illinois Subclass Members' Private Information; and

d. failing to take proper action following the Data Breaches to enact adequate privacy and security measures and protect Plaintiff Hohenbery and the Illinois Subclass Members' Private Information and other personal information from further unauthorized disclosure, release, data breaches, and theft.

149. In addition, Apria's failure to disclose that its computer systems were not well-protected and that Plaintiff Hohenbery and the Illinois Subclass Members' sensitive information was vulnerable and susceptible to intrusion and cyberattacks constitutes deceptive and/or unfair acts or practices because Apria knew such facts would (a) be unknown to and not easily discoverable by Plaintiff Hohenbery and the Illinois Subclass; and (b) defeat Plaintiff Hohenbery and the Illinois Subclass Members' ordinary, foreseeable and reasonable expectations concerning the security of their Private Information on Apria's servers.

150. Apria intended that Plaintiff Garrett and the Illinois Subclass Members rely on its deceptive and unfair acts and practices, misrepresentations, and the concealment, suppression, and omission of material facts, in connection with Apria's offering of goods and services and incorporating Plaintiff Garrett and the Illinois Subclass Members' PII on its servers, in violation of the Illinois CFA.

151. Apria also engaged in unfair acts and practices by failing to maintain the privacy and security of Plaintiff Hohenbery and the Illinois Subclass Members' Private Information, in violation of duties imposed by and public policies reflected in applicable federal and state laws, resulting in the data breach. These unfair acts and practices violated duties imposed by laws including the Federal Trade Commission Act (15 U.S.C. § 45) and similar state laws.

152. Apria's wrongful practices occurred in the course of trade or commerce.

153. Apria's wrongful practices were and are injurious to the public interest because those practices were part of a generalized course of conduct on the part of Apria that applied to Plaintiff Hohenbery and all Illinois Subclass Members and were repeated continuously before and after Apria obtained sensitive Private Information and other information from Plaintiff Hohenbery and the Illinois Subclass Members. Plaintiff Hohenbery and all Illinois Subclass Members were adversely affected by Apria's conduct and the public was and is at risk as a result thereof.

154. Apria also violated 815 Ill. Comp. Stat. § 505/2 by failing to immediately notify affected customers of the nature and extent of the Data Breach pursuant to the Illinois Personal Information Protection Act, 815 Ill. Comp. Stat. § 530/1, et. seq., which provides, at Section 10:

> Notice of Breach.
> Any data collector that owns or licenses personal information concerning an Illinois resident shall notify the resident at no charge that there has been a breach of the security of the system data following discovery or notification of the breach. The disclosure notification shall be made in the most expedient time to determine the scope of the breach and restore the reasonable integrity, security and confidentiality of the data system.

155. 815 Ill. Comp. Stat. § 530/20 provides that a violation of 815 Ill. Comp. Stat. § 530/10 "constitutes an unlawful practice under the Consumer Fraud and Deceptive Business Practices Act."

156. As a result of Apria's wrongful conduct, Plaintiff Hohenbery and the Illinois Subclass Members were injured in that they never would have allowed their sensitive Private

Information – the value of which Plaintiff and the Illinois Subclass Members no long have control – to be provided to Apria if they had been told or knew that Apria failed to maintain sufficient security to keep such data from being hacked and taken by others.

157. Apria's unfair and/or deceptive conduct proximately caused Plaintiff Hohenbery and the Illinois Subclass Members' injuries because, had Apria maintained customer Private Information with adequate security, Plaintiff Hohenbery and the Illinois Subclass Members would not have lost it.

158. As a direct and proximate result of Apria's conduct, Plaintiff Hohenbery and the Illinois Subclass Members have suffered harm, including but not limited to loss of time and money resolving fraudulent charges; loss of time and money obtaining protections against future identity theft; financial losses related to the purchases made at Apria that Plaintiff Hohenbery and the Illinois Subclass Members would have never made had they known of Apria's careless approach to cybersecurity; lost control over the value of Private Information; unreimbursed losses relating to fraudulent charges; losses relating to exceeding credit and debit card limits and balances; harm resulting from damaged credit scores and information; and other harm resulting from the unauthorized use or threat of unauthorized use of stolen Private Information, entitling them to damages in an amount to be proven at trial.

159. Pursuant to 815 Ill. Comp. Stat. § 505/10a(a), Plaintiff Hohenbery and the Illinois Subclass Members seeks actual, compensatory, and punitive damages (pursuant to 815 ILL. COMP. STAT. § 505/10a(c)), injunctive relief, and court costs and attorneys' fees as a result of Apria's violations of the Illinois CFA.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of himself and the Class described above, seeks the following relief:

a. An order certifying this action as a class action under Fed. R. Civ. P. 23, defining the classes as requested herein, appointing the undersigned as Class counsel, and finding that Plaintiff are proper representatives of the Classes requested herein;

b. Judgment in favor of Plaintiff and the Class Members awarding them appropriate monetary relief, including actual damages, statutory damages, equitable relief, restitution, disgorgement, and statutory costs;

c. An order providing injunctive and other equitable relief as necessary to protect the interests of the Classes as requested herein;

d. An order instructing Apria to purchase or provide funds for credit monitoring services for Plaintiff and all Class Members;

e. An order requiring Apria to pay the costs involved in notifying the Class Members about the judgment and administering the claims process;

f. A judgment in favor of Plaintiff and the Classes awarding them pre-judgment and post judgment interest, reasonable attorneys' fees, costs and expenses as allowable by law, and

g. An award of such other and further relief as this Court may deem just and proper.

///

///

///

DEMAND FOR JURY TRIAL

Plaintiff demands a trial by jury on all triable issues.

DATED: June 20, 2023

Respectfully submitted,

/s/ M. Anderson Berry

M. Anderson Berry
CLAYEO C. ARNOLD
A PROFESSIONAL CORPORATION
865 Howe Avenue
Sacramento, CA 95825
Telephone: (916) 239-4778
Fax: (916) 924-1829
aberry@justice4you.com

MARKOVITS, STOCK & DEMARCO, LLC
Terence R. Coates (*Pro Hac Vice Forthcoming*)
Dylan J. Gould *Pro Hac Vice Forthcoming*)
119 E. Court Street, Suite 530
Cincinnati, OH 45202
Telephone: (513) 651-3700
Fax: (513) 665-0219
tcoates@msdlegal.com
dgould@msdlegal.com

Counsel for Plaintiff and the Proposed Class

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

CHAD HOHENBERY, individually, and on behalf of all others similarly situated,

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

(c) Attorneys *(Firm Name, Address, and Telephone Number)*
M. Anderson Berry, CLAYEO C. ARNOLD, APC
865 Howe Avenue Sacramento, CA 95825
Tel: (916) 239-4778; aberry@justice4you.com

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

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

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

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

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

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. Sec. 1332(d)(2) and (3); 28 U.S.C. Sec. 1391(b)(2)

Brief description of cause:
Class Action Data Breach

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 Hon. Richard L. Young DOCKET NUMBER 1:23-cv-01003-RLY-KMB

DATE 06/20/2023

SIGNATURE OF ATTORNEY OF RECORD /s/ M. Anderson Berry

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

CHAD HOHENBERY, individually, and on behalf of all others similarly situated,

Plaintiff(s)

v.

APRIA HEALTHCARE LLC

Defendant(s)

Civil Action No. 1:23-cv-1074

SUMMONS IN A CIVIL ACTION

To: *(Defendant's name and address)* APRIA HEALTHCARE LLC
7353 COMPANY DRIVE
INDIANAPOLIS, IN 46237

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:

M. Anderson Berry
CLAYEO C. ARNOLD, A PROFESSIONAL CORPORATION
865 Howe Avenue
Sacramento, CA 95825
Telephone: (916) 239-4778
aberry@justice4you.com

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. 1:23-cv-1074

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:

Print Save As... Reset