EXHIBIT A(7)

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

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

Plaintiff Anthony Boyd ("Plaintiff"), individually and on behalf of classes of similarly situated individuals (defined below), brings this action against Defendant Apria Healthcare LLC ("Apria" or "Defendant"). Plaintiff makes the following allegations based upon personal knowledge as to his own actions and upon information and belief as to all other matters, and he believes that reasonable discovery will provide additional evidentiary support for the allegations herein.

I. NATURE OF THE CASE

1. Apria provides home healthcare equipment to nearly 2 million patients across the United States.[1] Among its major services and products, Apria offers assistance for patients struggling with sleep problems, COPD and breathing difficulties, and diabetes, among other health problems.

2. Apria's patients entrust Apria with their personally identifiable information ("PII") and protected health information ("PHI") to obtain Apria's services. Just three years ago,

[1] *See* https://www.apria.com/about-us.

Apria was touting its "leadership position in the healthcare industry" as a result of its decision to "set[] and maintain[] stringent requirements needed to achieve HIPAA compliance across its patient data platform."[2]

3. But while it was holding itself out to the public as a leader in keeping its patients' data private, Apria in reality allowed that data to be accessed by third parties. More troublingly, Apria was aware as early as September 1, 2021—nearly two years ago—that its systems had been compromised by an unauthorized third party. Yet it waited years to notify its patients that their data had been compromised.

4. On or about May 22, 2023, Apria finally admitted that an unauthorized individual accessed its systems between April 5, 2019 and May 7, 2019, and again from August 27, 2021 to October 10, 2021 (the "Data Breach"). Over 1.8 million patients' most private information—including personal, medical, health insurance, and financial information, as well as Social Security numbers—was compromised in the Data Breach.

5. Plaintiff now seeks compensation under principles of common law negligence and unjust enrichment, as well as for breach of the California Confidentiality of Medical Information Act and Unfair Competition Law, for his damages and those of fellow Class members. Plaintiff also seeks injunctive relief to ensure that Apria cannot continue to put its patients at risk.

II. JURISDICTION AND VENUE

6. This Court has jurisdiction over this action under the Class Action Fairness Act ("CAFA"), 28 U.S.C. § 1332(d), because the aggregate amount in controversy exceeds

[2] *See* Louis Columbus, *How Absolute Protects Patient Data at Apria* Healthcare, FORBES (Mar. 15, 2020), *available at* https://www.forbes.com/sites/louiscolumbus/2020/03/15/how-absolute-protects-patient-data-at-apria-healthcare/?sh=2f7a35263cb9 (last visited June 20, 2023).

$5,000,000, exclusive of interests and costs, there are more than 100 Class members, and one or more members of the classes are residents of a different state than the Defendant. The Court also has supplemental jurisdiction over the state law claims under 28 U.S.C. § 1367.

7. This Court has personal jurisdiction over Defendant because it is headquartered in this District.

8. Venue is proper in this District pursuant to 28 U.S.C. §§ 1391(b), as Defendant resides, transacts business, committed an illegal or tortious act, has an agent, and/or can be found in this District.

III. PARTIES

9. Plaintiff Anthony Boyd is a resident of Menifee, California and is a former customer of Apria Healthcare. Mr. Boyd received a telephone call from Apria informing him that his PHI was accessed without authorization in the Data Breach.

10. Defendant, Apria Healthcare LLC, is a Delaware corporation headquartered in this District at 7353 Company Drive, Indianapolis, Indiana 46237. Defendant collects and maintains the personal information of millions of U.S. consumers.

11. Defendant's unlawful conduct was authorized, ordered, or performed by its directors, officers, managers, agents, employees, or representatives in the course of their employment and while actively engaged in the management of Defendant's affairs.

IV. FACTUAL ALLEGATIONS

A. The Data Breach

12. As outlined above, Apria admitted it was the subject of a massive data breach that affected millions of its customers. Between April 5, 2019 and May 7, 2019 and again between August 27, 2021 and October 10, 2021, unauthorized third-party cybercriminals infiltrated the

network that Apria uses to store sensitive personal information (including PII and PHI) of its customers. These cybercriminals went undetected as they accessed PII and PHI over the course of several months in 2019 and 2021.

13. The customer PII and PHI the hackers accessed include names, Social Security numbers, personal details, medical records, health insurance information, and financial data. The financial data accessed includes account numbers, credit/debit card numbers, account security codes, access codes, passwords, and PINs.

14. Apria inexplicably waited until 2023, however, to begin notifying its customers that their PII and PHI was compromised in the Data Breach. In fact, some customers were unaware for over *four years* that their PII and PHI had been compromised.

15. Apria had obligations to Plaintiff and to Class members to safeguard their PII and PHI and to protect it from unauthorized access and disclosure. Indeed, Plaintiff and Class members provided their PII and PHI to Apria with the reasonable expectation and mutual understanding that Apria would comply with its obligations to keep such information confidential and secure from unauthorized access. Apria's data security obligations were particularly important given the substantial increase in cyberattacks and/or data breaches of major companies before the Data Breach.

16. Apria also promises to keep its customers' PII and PHI secure, as it is legally required to do under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"). In its Privacy Policy and HIPAA Privacy Notice, Apria promises that it "maintain[s] commercially reasonable security measures to protect the Personally Identifiable Information we

collect and store from loss, misuse, or unauthorized access."[3] While Apria goes on to claim that it cannot "guarantee absolute security," it again avers that it "strive[s] to use commercially acceptable means to protect your Personally Identifiable Information."[4]

17. As a result of the Data Breach, numerous data security experts are suggesting that affected consumers take steps to protect their identities.

B. Plaintiff Expected Apria to Keep His Information Secure.

18. Plaintiff Anthony Boyd is a former customer of Apria.

19. As a condition of receiving products and services from Apria, Mr. Boyd provided his PII and PHI to Defendant, which Defendant then stored and maintained.

20. Mr. Boyd places significant value on the security of his PII and PHI, especially when receiving health services or health insurance services. He entrusted his sensitive PII and PHI to Apria with the understanding that Apria would keep his information secure and employ reasonable and adequate security measures to ensure that it would not be compromised.

21. Additionally, Plaintiff is very careful about sharing his PII and PHI. He has never knowingly transmitted unencrypted PII or PHI over the internet or any other unsecured source.

22. A couple of months ago, Mr. Boyd received a phone call from Apria Healthcare. The person he spoke to informed him that, as a result of a data breach at Apria, his health care information at Apria had been compromised. The caller informed him that Apria would be offering him free credit monitoring and told him to look out for a letter from Apria with more information.

---

[3] *See* Privacy Policy, APRIA, *available at* https://www.apria.com/privacy-policy#:~:text=We%20do%20not%20disclose%20personal,for%20their%20direct%20marketing%20purposes.

[4] *Id.*

23. As a result of Apria's exposure of Mr. Boyd's PII and PHI, he will have to spend hours attempting to mitigate the affects of the Data Breach, including monitoring financial and other important accounts for fraudulent activity.

24. Given the highly-sensitive nature of the information that was compromised, Mr. Boyd has already suffered injury and remains at a substantial and imminent risk of future harm. In addition, Mr. Boyd has a continuing interest in ensuring that his PII and PHI, which, upon information and belief, remains in Defendant's possession, is protected and safeguarded from future breaches.

C. FTC Security Guidelines Concerning PII

25. The Federal Trade Commission ("FTC") has established security guidelines and recommendations to help entities protect PII and reduce the likelihood of data breaches.

26. Section 5 of the FTC Act, 15 U.S.C. § 45, prohibits "unfair . . . practices in or affecting commerce," including, as interpreted by the FTC, failing to use reasonable measures to protect PII by companies like Defendant. Several publications by the FTC outline the importance of implementing reasonable security systems to protect data. The FTC has made clear that protecting sensitive customer data should factor into virtually all business decisions.

27. In 2016, the FTC provided updated security guidelines in a publication titled *Protecting Personal Information: A Guide for Business*. Under these guidelines, companies should protect consumer information they keep; limit the sensitive consumer information they keep; encrypt sensitive information sent to third parties or stored on computer networks; identify and understand network vulnerabilities; regularly run up-to-date anti-malware programs; and pay particular attention to the security of web applications—the software used to inform visitors to a company's website and to retrieve information from the visitors.

28. The FTC recommends that businesses do not maintain payment card information beyond the time needed to process a transaction; restrict employee access to sensitive customer information; require strong passwords be used by employees with access to sensitive customer information; apply security measures that have proven successful in the particular industry; and verify that third parties with access to sensitive information use reasonable security measures.

29. The FTC also recommends that companies use an intrusion detection system to immediately expose a data breach; monitor incoming traffic for suspicious activity that indicates a hacker is trying to penetrate the system; monitor for the transmission of large amounts of data from the system; and develop a plan to respond effectively to a data breach in the event one occurs.

30. The FTC has brought several actions to enforce Section 5 of the FTC Act. According to its website:

> When companies tell consumers they will safeguard their personal information, the FTC can and does take law enforcement action to make sure that companies live up these promises. The FTC has brought legal actions against organizations that have violated consumers' privacy rights, or misled them by failing to maintain security for sensitive consumer information, or caused substantial consumer injury. In many of these cases, the FTC has charged the defendants with violating Section 5 of the FTC Act, which bars unfair and deceptive acts and practices in or affecting commerce. In addition to the FTC Act, the agency also enforces other federal laws relating to consumers' privacy and security.[5]

31. Apria was aware or should have been aware of its obligations to protect its customers' PII, PHI, and privacy before and during the Data Breach, yet failed to take reasonable steps to protect customers from unauthorized access. Among other violations, Apria violated its obligations under Section 5 of the FTC Act.

---

[5] *Privacy and Security Enforcement*, Fed. Trade Comm'n, https://www.ftc.gov/news-events/topics/protecting-consumer-privacy-security/privacy-security-enforcement.

D. Apria Was on Notice of Data Threats and the Inadequacy of Its Data Security.

32. Apria was on notice that companies maintaining large amounts of PII and PHI during their regular course of business are prime targets for criminals looking to gain unauthorized access to sensitive and valuable information, such as the type of data at issue in this case.

33. At all relevant times, Apria knew, or should have known, that the PII and PHI that it collected was a target for malicious actors. Despite such knowledge, and well-publicized cyberattacks on similar companies, Apria failed to implement and maintain reasonable and appropriate data privacy and security measures to protect Plaintiff's and Class members' PII and PHI from cyber-attacks that Apria should have anticipated and guarded against.

34. It is well known among companies that store PII and PHI that sensitive information—such as the Social Security numbers and health information accessed in the Data Breach—is valuable and frequently targeted by criminals. In a recent article, *Business Insider* noted that "[d]ata breaches are on the rise for all kinds of businesses, including retailers . . . . Many of them were caused by flaws in . . . systems either online or in stores."[6]

35. In light of recent high profile data breaches, including Microsoft (250 million records, December 2019), T-Mobile (110 million records, August 2021), Wattpad (268 million records, June 2020), Facebook (267 million users, April 2020), Estee Lauder (440 million records, January 2020), Whisper (900 million records, March 2020), and Advanced Info Service (8.3 billion records, May 2020), Apria knew or should have known that its electronic records would be targeted by cybercriminals.

---

[6] Dennis Green, Mary Hanbury & Aine Cain, *If you bought anything from these 19 companies recently, your data may have been stolen*, BUSINESS INSIDER (Nov. 19, 2019, 8:05 A.M.), https://www.businessinsider.com/data-breaches-retailers-consumer-companies-2019-1 (last visited Feb. 16, 2023).

36. Indeed, cyberattacks have become so notorious that the FBI and U.S. Secret Service have issued a warning to potential targets so they are aware of, take appropriate measures to prepare for, and are able to thwart such an attack.

E. The Data Breach Harmed Plaintiff and Class Members

37. Plaintiff and Class members have suffered and will continue to suffer harm because of the Data Breach.

38. Plaintiff and Class members face an imminent and substantial risk of injury of identity theft and related cyber crimes due to the Data Breach. Once data is stolen, malicious actors will either exploit the data for profit themselves or sell the data on the dark web to someone who intends to exploit the data for profit. Hackers would not incur the time and effort to steal PII and PHI—thereby risking prosecution by listing it for sale on the dark web—if the PII and PHI was not valuable to malicious actors.

39. The dark web helps ensure users' privacy by effectively hiding server or IP details from the public. Users need special software to access the dark web. Most websites on the dark web are not directly accessible via traditional searches on common search engines and are therefore accessible only by users who know the addresses for those websites.

40. Malicious actors use PII and PHI to gain access to Class members' digital life, including bank accounts, social media, and credit card details. During that process, hackers can harvest other sensitive data from the victim's accounts, including personal information of family, friends, and colleagues.

41. Consumers are injured every time their data is stolen and placed on the dark web, even if they have been victims of previous data breaches. Not only is the likelihood of identity theft increased, but the dark web is not like Google or eBay. It is comprised of

multiple discrete repositories of stolen information. Each data breach puts victims at risk of having their information uploaded to different dark web databases and viewed and used by different criminal actors.

42. Apria issued misleading public statements about the Data Breach, including its data breach notification letters,[7] in which it attempts to downplay the seriousness of the Data Breach by stating that hackers were likely Apria's funds, not after its customers' data. Apria concluded that "There is no evidence of funds removed, and Apria is not aware of the misuse of personal information related to this incident."

43. Apria's intentionally misleading public statements ignore the serious harm its security flaws caused to the Class. Worse, those statements could convince Class members that they do not need to take steps to protect themselves.

44. The data security community agrees that the PII and PHI compromised in the Data Breach greatly increases Class members' risk of identity theft and fraud.

45. As Justin Fier, senior vice president for AI security company Darktrace, observed following a recent data breach at T-Mobile, "[t]here are dozens of ways that the information that was stolen could be weaponized." He added that such a massive treasure trove of consumer profiles could be of use to everyone from nation-state hackers to criminal syndicates.[8]

---

[7] *Available at* https://apps.web.maine.gov/online/aeviewer/ME/40/bf218a4e-1ffd-4f14-a74d-3d34aec8d6c7/bde05c1a-c231-42a5-89b5-6141c2c33f9f/document.html

[8] https://www.cnet.com/tech/services-and-software/t-mobile-gets-hacked-again-is-the-un-carrier-un-safe/.

46. Criminals can use the PII and PHI that Apria lost to target Class members for imposter scams, a type of fraud initiated by a person who pretends to be someone the victim can trust in order to steal sensitive data or money.[9]

47. Criminals can also use the PII and PHI that Apria lost to commit medical identity theft.[10] These third parties can use an individual's name, Social Security number, health insurance information, or some combination thereof to see a doctor, get prescriptions, fraudulently submit claims to an individual's insurance provider, or get medical care—which could impact Plaintiff's or Class members' ability to access their own medical care or health insurance benefits, not to mention their credit.

48. The PII and PHI accessed in the Data Breach therefore has significant value to the hackers that have already sold or attempted to sell that information and may do so again.

49. Malicious actors can use Class members' PII to open new financial accounts, open new utility accounts, obtain medical treatment using victims' health insurance, file fraudulent tax returns, obtain government benefits, obtain government IDs, or create "synthetic identities."

50. As established above, the PII and PHI accessed in the Data Breach is also very valuable to Apria. Apria collects, retains, and uses this information to increase profits through predictive and other targeted marketing campaigns. Apria customers value the privacy of this information and expect Apria to allocate enough resources to ensure it is adequately protected. Customers would not have done business with Apria, provided their PII, PHI, and payment card information, and/or paid the same prices for Apria's goods and services had they known Apria did not implement reasonable security measures to protect their PII and PHI. Apria states that its

---

9 *See* https://consumer.ftc.gov/features/imposter-scams.

10 *See* https://consumer.ftc.gov/articles/what-know-about-medical-identity-theft.

mission is to "Improv[e] the Quality of Life for Our Patients at Home."[11] Customers expect that the payments they make to Apria incorporate the costs to implement reasonable security measures to protect customers' PII and PHI as part of improving their "quality of life."

51. Indeed, "[f]irms are now able to attain significant market valuations by employing business models predicated on the successful use of personal data within the existing legal and regulatory frameworks."[12] American companies are estimated to have spent over $19 billion on acquiring personal data of consumers in 2018.[13] It is so valuable to identity thieves that once PII has been disclosed, criminals often trade it on the "cyber black-market" or the "dark web" for many years.

52. As a result of their real and significant value, identity thieves and other cyber criminals have openly posted credit card numbers, Social Security numbers, PII, and other sensitive information directly on various Internet websites, making the information publicly available. This information from various breaches, including the information exposed in the Data Breach, can be readily aggregated and become more valuable to thieves and more damaging to victims.

53. The PII and PHI accessed in the Data Breach is also very valuable to Plaintiff and Class members. Consumers often exchange personal information for goods and services. For example, consumers often exchange their personal information for access to wifi in places like airports and coffee shops. Likewise, consumers often trade their names and email

---

[11] *See* https://www.apria.com/about-us.

[12] OECD, *Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value*, OECD DIGITAL ECONOMY PAPERS, No. 220, Apr. 2, 2013, https://doi.org/10.1787/5k486qtxldmq-en.

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

addresses for special discounts (*e.g.*, sign-up coupons exchanged for email addresses). Consumers use their unique and valuable PII to access the financial sector, including when obtaining a mortgage, credit card, or business loan. As a result of the Data Breach, Plaintiff and Class members' PII and PHI has been compromised and lost significant value.

54. Consumers place a high value on the privacy of that data, as they should. Researchers shed light on how much consumers value their data privacy—and the amount is considerable. Indeed, studies confirm that "when privacy information is made more salient and accessible, some consumers are willing to pay a premium to purchase from privacy protective websites."[14]

55. Given these facts, any company that transacts business with a consumer and then compromises the privacy of consumers' PII and PHI has thus deprived that consumer of the full monetary value of the consumer's transaction with the company.

56. Plaintiff and Class members will face a risk of injury due to the Data Breach for years to come. Malicious actors often wait months or years to use the personal information obtained in data breaches, as victims often become complacent and less diligent in monitoring their accounts after a significant period has passed. These bad actors will also re-use stolen personal information, meaning individuals can be the victim of several cyber crimes stemming from a single data breach. Finally, there is often significant lag time between when a person suffers harm due to theft of their PII and PHI and when they discover the harm. For example, victims rarely know that certain accounts have been opened in their name until contacted by collections agencies. Plaintiff and Class members will therefore need to

[14] Janice Y. Tsai et al., *The Effect of Online Privacy Information on Purchasing Behavior*, *An Experimental Study*, 22(2) INFO. SYS. RES. 254 (June 2011) https://www.jstor.org/stable/23015560?seq=1.

continuously monitor their accounts for years to ensure their PII and PHI obtained in the Data Breach is not used to harm them.

57. Even when reimbursed for money stolen due to a data breach, consumers are not made whole because the reimbursement fails to compensate for the significant time and money required to repair the impact of the fraud.

58. Victims of identity theft also experience harm beyond economic effects. According to a 2018 study by the Identity Theft Resource Center, 32% of identity theft victims experienced negative effects at work (either with their boss or coworkers) and 8% experienced negative effects at school (either with school officials or other students).

59. The U.S. Government Accountability Office likewise determined that "stolen data may be held for up to a year or more before being used to commit identity theft," and that "once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years."

60. Plaintiff and Class member customers have failed to receive the value of the Apria services for which they paid and/or would have paid less had they known that Apria was failing to use reasonable security measures to secure their data.

F. Defendant Failed to Take Reasonable Steps to Protect its Customers' PII

61. Apria requires its customers to provide a significant amount of highly personal and confidential PII and PHI to purchase its good and services. Apria collects, stores, and uses this data to maximize profits while failing to encrypt or protect it properly.

62. Apria has legal duties to protect its customers' PII and PHI by implementing reasonable security features. This duty is further defined by federal and state guidelines and laws, including HIPAA, as well as industry norms.

63. Defendant breached its duties by failing to implement reasonable safeguards to ensure Plaintiff's and Class members' PII and PHI was adequately protected. As a direct and proximate result of this breach of duty, the Data Breach occurred, and Plaintiff and Class members were harmed. Plaintiff and Class members did not consent to having their PII and PHI disclosed to any third-party, much less a malicious hacker who could exfiltrate it and then sell it to criminals on the dark web.

64. Defendant could have prevented this Data Breach by properly securing and encrypting the systems containing the PII and PHI of Plaintiff and Class members. Alternatively, Defendant could have destroyed the data, especially for individuals with whom it had not had a relationship for a period of time or for whom there was no reasonably anticipated future use.

65. Defendant's negligence in safeguarding the PII and PHI of Plaintiff and Class members is exacerbated by the repeated warnings and alerts directed to companies like Defendant to protect and secure sensitive data they possess.

66. Experts have identified several best practices that business like Apria should implement at a minimum, including, but not limited to: educating all employees; requiring strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data; and limiting which employees can access sensitive data.

67. Other best cybersecurity practices include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers;

monitoring and protection of physical security systems; protection against any possible communication system; and training staff regarding critical points.

68. Defendant failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

69. The foregoing frameworks are existing and applicable industry standards, and Defendant failed to comply with these accepted standards, thereby opening the door to and causing the Data Breach.

70. Upon information and belief, Defendant failed to comply with one or more of the foregoing industry standards, as evidenced by the Data Breach and the unreasonable length of time between the unauthorized access to Apria's systems and Apria's discovery of that unauthorized access.

71. The Data Breach was a reasonably foreseeable consequence of Defendant's inadequate security systems. Apria, which has approximately 2 million patients serviced from its hundreds of locations, certainly has the resources to implement reasonable security systems to prevent or limit damage from data breaches. Even so, Apria failed to properly invest in its data security. Had Apria implemented reasonable data security systems and procedures (*i.e.*, followed guidelines from industry experts and state and federal governments), then it likely could have prevented hackers from infiltrating its systems and accessing its customers' PII and PHI.

72. Apria's failure to implement reasonable security systems has caused Plaintiff and Class members to suffer and continue to suffer harm that adversely impact Plaintiff and

Class members economically, emotionally, and/or socially. As discussed above, Plaintiff and Class members now face a substantial, imminent, and ongoing threat of identity theft, scams, and resulting harm. These individuals now must spend significant time and money to continuously monitor their accounts and credit scores and diligently sift out phishing communications to limit potential adverse effects of the Data Breach, regardless of whether any Class member ultimately falls victim to identity theft.

73. In sum, Plaintiff and Class members were injured as follows: (i) theft of their PII and PHI and the resulting loss of privacy rights in that information; (ii) improper disclosure of their PII and PHI; (iii) the lost value of unauthorized access to their PII and PHI; (iv) diminution in value of their PII and PHI; (v) the certain, imminent, and ongoing threat of fraud and identity theft, including the economic and non-economic impacts that flow therefrom; (vi) ascertainable out-of-pocket expenses and the value of their time allocated to fixing or mitigating the effects of the Data Breach; (vii) overpayments to Apria for goods and services purchased, as Plaintiff and Class members reasonably believed a portion of the sale price would fund reasonable security measures that would protect their PII and PHI, which was not the case; and/or (viii) nominal damages.

74. Even though Apria has decided to offer free credit monitoring for one year to its affected customers, this is insufficient to protect Plaintiff and Class members. As discussed above, the threat of identity theft and fraud from the Data Breach will extend for many years and cost Plaintiff and the Classes significant time and effort.

75. Plaintiff and Class members therefore have a significant and cognizable interest in obtaining injunctive and equitable relief (in addition to any monetary damages) that protects them from these long-term threats. Accordingly, this action represents the enforcement of an

important right affecting the public interest and will confer a significant benefit on the general public or a large class of persons.

V. CLASS ALLEGATIONS

76. Plaintiff brings this action on behalf of himself and all others similarly situated pursuant to Federal Rule of Civil Procedure 23 as representative of the Classes defined as follows:

(a) **The Nationwide Class:** All U.S. residents whose data was accessed in the Data Breach.

(b) **The California Subclass:** All California residents whose data was accessed in the Data Breach.

77. Specifically excluded from the Classes are Defendant; its officers, directors, or employees; any entity in which Defendant has a controlling interest; and any affiliate, legal representative, heir, or assign of Defendant. Also excluded from the Classes are any federal, state, or local governmental entities, any judicial officer presiding over this action and the members of their immediate family and judicial staff, and any juror assigned to this action.

78. Class Identity: The members of the Classes are readily identifiable and ascertainable. Defendant and/or its affiliates, among others, possess the information to identify and contact Class members.

79. Numerosity: The members of the Classes 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 Nationwide Class of approximately 1,869,598 individuals whose data was compromised in the Data Breach, and the California Class consists of hundreds of thousands of customers whose data was compromised in the Data Breach.

80. Typicality: Plaintiff's claims are typical of the claims of the members of the classes because all Class members had their PII and PHI accessed in the Data Breach and were harmed as a result.

81. Adequacy: Plaintiff will fairly and adequately protect the interests of the Classes. Plaintiff has no interest antagonistic to those of the classes and is aligned with Class members' interests because Plaintiff was subject to the same Data Breach as Class members and faces similar threats due to the Data Breach as Class members. Plaintiff has also retained competent counsel with significant experience litigating complex class actions, including Data Breach cases involving multiple classes.

82. Commonality and Predominance: There are questions of law and fact common to the classes. These common questions predominate over any questions affecting only individual Class members. The common questions of law and fact include, without limitation:

a. Whether Defendant owed Plaintiff and Class members a duty to implement and maintain reasonable security procedures and practices to protect their personal information;

b. Whether Defendant received a benefit without proper restitution, making it unjust for Defendant to retain the benefit without commensurate compensation;

c. Whether Defendant acted negligently in connection with the monitoring and/or protection of Plaintiff's and Class members' PII;

d. Whether Defendant breached its duty to implement reasonable security systems to protect Plaintiff's and Class members' PII;

e. Whether Defendant's breach of its duty to implement reasonable security systems directly and/or proximately caused damages to Plaintiff and Class members;

f. Whether Defendant adequately addressed and fixed the vulnerabilities that enabled the Data Breach;

g. When Defendant learned of the Data Breach and whether its response was adequate;

h. Whether Plaintiff and other Class members are entitled to credit monitoring and other injunctive relief;

i. Whether Defendant provided timely notice of the Data Breach to Plaintiff and Class members; and,

j. Whether Class members are entitled to compensatory damages, punitive damages, and/or statutory or civil penalties as a result of the Data Breach.

83. Defendant has engaged in a common course of conduct, and Class members have been similarly impacted by Defendant's failure to maintain reasonable security procedures and practices to protect customers' PII and PHI, as well as Defendant's failure to timely alert affected customers to the Data Breach.

84. 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 if not all Class members would find the cost of litigating their individual claims prohibitively high and 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 and risk inconsistent treatment of claims arising from the same set of facts and occurrences.

Plaintiff knows of no difficulty likely to be encountered in the maintenance of this action as a class action under Federal Rule of Civil Procedure 23.

VI. CLAIMS FOR RELIEF

COUNT I
Negligence
(On Behalf of Plaintiff and the Nationwide Class or Alternatively State-Specific Subclasses)

85. Plaintiff repeats and realleges every allegation set forth in the preceding paragraphs.

86. Defendant owed Plaintiff and Class members a duty to exercise reasonable care in protecting their PII and PHI from unauthorized disclosure or access. Defendant breached its duty of care by failing to implement reasonable security procedures and practices to protect this PII and PHI. Among other things, Defendant failed to: (i) implement security systems and practices consistent with federal and state laws and guidelines; (ii) implement security systems and practices consistent with industry norms; (iii) timely detect the Data Breach; and (iv) timely disclose the Data Breach to impacted customers.

87. Defendant knew or should have known that Plaintiff's and Class members' PII and PHI was highly sought after by cyber criminals and that Plaintiff and Class members would suffer significant harm if their PII and PHI was compromised by hackers.

88. Defendant also knew or should have known that timely detection and disclosure of the Data Breach was required and necessary to allow Plaintiff and Class members to take appropriate actions to mitigate the resulting harm. These efforts include, but are not limited to, freezing accounts, changing passwords, monitoring credit scores/profiles and their health

insurance carriers for fraudulent charges, contacting financial institutions, and cancelling or monitoring government-issued IDs such as passports and driver's licenses.

89. Defendant had a special relationship with Plaintiff and Class members who entrusted Defendant with several pieces of PII and PHI. Defendant's customers were required to provide PII and PHI when purchasing or attempting to purchase Defendant's products and services. Plaintiff and Class members were led to believe Defendant would take reasonable precautions to protect their PII and PHI and would timely inform them if their PII and PHI was compromised, which Defendant failed to do.

90. The harm that Plaintiff and Class members suffered (and continue to suffer) was the reasonably foreseeable product of Defendant's breach of its duty of care. Defendant failed to enact reasonable security procedures and practices, and Plaintiff and Class members were the foreseeable victims of data theft that exploited the inadequate security measures. The PII and PHI accessed in the Data Breach is precisely the type of information that cyber criminals seek and use to commit cyber crimes.

91. But-for Defendant's breach of its duty of care, the Data Breach would not have occurred and Plaintiff's and Class members' PII and PHI would not have been accessed by an unauthorized and malicious party.

92. As a direct and proximate result of the Defendant's negligence, Plaintiff and Class members have been injured and are entitled to damages in an amount to be proven at trial. Such damages include one or more of the following: ongoing, imminent, certainly impending threat of identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; loss of the value of their privacy and the confidentiality of the

compromised PII and PHI; illegal sale of the compromised PII and PHI on the black market; mitigation expenses and time spent on credit monitoring, identity theft insurance, and credit freezes and unfreezes; time spent in response to the Data Breach reviewing bank statements, credit card statements, and credit reports; expenses and time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; lost value of their PII and PHI; lost value of unauthorized access to their PII and PHI; lost benefit of their bargains and overcharges for services; and other economic and non-economic harm.

COUNT II
Negligence *Per Se*

(On Behalf of Plaintiff and the Nationwide Class or Alternatively State-Specific Subclasses)

93. Plaintiff repeats and realleges every allegation set forth in the preceding paragraphs.

94. Section 5 of the FTC Act, 15 U.S.C. § 45, prohibits "unfair . . . practices in or affecting commerce" including, as interpreted and enforced by the FTC, the unfair act or practice by Defendant of failing to use reasonable measures to protect PII. Various FTC publications and orders also form the basis of Defendant's duty.

95. Defendant violated Section 5 of the FTC Act (and similar state statutes) by failing to use reasonable measures to protect PII and PHI and not complying with industry standards. Defendant's conduct was particularly unreasonable given the nature and amount of PII and PHI obtained and stored and the foreseeable consequences of a data breach on Defendant's systems.

96. Defendant's violation of Section 5 of the FTC Act (and similar state statutes) constitutes negligence *per se*.

97. Plaintiff and Class members are consumers within the class of persons Section 5 of the FTC Act (and similar state statutes) were intended to protect.

98. Moreover, the harm that has occurred is the type of harm the FTC Act (and similar state statutes) was intended to guard against. Indeed, the FTC has pursued over fifty 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 suffered by Plaintiff and Class members.

99. As a direct and proximate result of the Defendant's negligence, Plaintiff and Class members have been injured and are entitled to damages in an amount to be proven at trial. Such damages include one or more of the following: ongoing, imminent, certainly impending threat of identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; loss of the value of their privacy and the confidentiality of the compromised PII and PHI; illegal sale of the compromised PII and PHI on the black market; mitigation expenses and time spent on credit monitoring, identity theft insurance, and credit freezes and unfreezes; time spent in response to the Data Breach reviewing bank statements, credit card statements, and credit reports; expenses and time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; lost value of their PII and PHI; lost value of unauthorized access to their PII and PHI; lost benefit of their bargains and overcharges for services; and other economic and non-economic harm.

COUNT III
Breach of California Confidentiality of Medical Information Act
Cal. Civ. Code § 56
(On Behalf of Plaintiff and the California Class)

100. Plaintiff repeats and realleges every allegation set forth in the preceding paragraphs.

101. Defendant is "a provider of health care," as defined in Cal. Civ. Code § 56.05(m) and is therefore subject to the requirements of the CMIA, Cal. Civ. Code § 56.10(a), (d) and (e), 56.36(b), 56.101(a) and (b).

102. At all relevant times, Defendant was a health care provider because it had the "purpose of maintaining medical information . . . in order to make the information available to an individual or to a provider of health care at the request of the individual or a provider of health care, for purposes of allowing the individual to manage his or her information, or for the diagnosis or treatment of the individual." *See* Cal. Civ. Code § 56.06(a).

103. As a provider of health care, Defendant is required by the CMIA to ensure that medical information regarding patients is not disclosed or disseminated or released without patient's authorization, and to protect and preserve the confidentiality of the medical information regarding a patient, under Civil Code §§ 56.06, 56.10, 56.13, 56.20, 56.245, 56.26, 56.35, 56.36, and 56.101.

104. As a provider of health care, Defendant is required by the CMIA not to disclose medical information regarding a patient without first obtaining an authorization under Civil Code §§ 56.06, 56.10, 56.13, 56.20, 56.245, 56.26, 56.35, and 56.104.

105. Plaintiff and Class members are "patients" as defined in CMIA, Cal. Civ. Code §56.05(k). Furthermore, Plaintiff and Class members, as patients and customers of Defendant, had their individually identifiable "medical information," within the meaning of Civil Code

§ 56.05(j), created, maintained, preserved, and stored by Defendant, and were patients on or before the date of the Data Breach.

106. Defendant disclosed "medical information," as defined in CMIA, Cal. Civ. Code § 56.05(j), to unauthorized persons without first obtaining consent, in violation of Cal. Civ. Code § 56.10(a). The disclosure of information to unauthorized individuals in the Data Breach resulted from the affirmative actions of Defendant's employees, which allowed the hackers to see and obtain Plaintiff's and Class members' medical information.

107. Defendant negligently created, maintained, preserved, stored, and then exposed Plaintiff's and Class members' individually identifiable "medical information," within the meaning of Cal. Civ. Code § 56.05(j), including Plaintiff's and Class members' first and last names, health insurance ID numbers, dates of birth, addresses, and other information, that alone or in combination with other publicly available information, reveals their identities. Specifically, Defendant knowingly allowed and affirmatively acted in a manner that allowed unauthorized parties to access and view Plaintiff's and Class members' confidential PHI.

108. Defendant's negligence resulted in the release of individually identifiable medical information pertaining to Plaintiff and Class members to unauthorized persons and the breach of the confidentiality of that information. Defendant's negligent failure to maintain, preserve, store, abandon, destroy, and/or dispose of Plaintiff's and Class members' medical information in a manner that preserved the confidentiality of the information contained therein, in violation of Cal. Civ. Code §§ 56.06 and 56.101(a).

109. Defendant also violated Sections 56.06 and 56.101 of the CMIA, which prohibit the negligent creation, maintenance, preservation, storage, abandonment, destruction or disposal of confidential personal medical information.

110. Plaintiff's and Class members' medical information was accessed and viewed by hackers and other unauthorized parties during and following the Data Breach.

111. Plaintiff's and Class members' medical information that was the subject of the Data Breach included "electronic medical records" or "electronic health records" as referenced by Civil Code § 56.101(c) and defined by 42 U.S.C. § 17921(5).

112. Defendant's computer systems did not protect and preserve the integrity of electronic medical information in violation of Cal. Civ. Code § 56.101(b)(1)(A). As a direct and proximate result of Defendant's above-noted wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused the Data Breach, and violation of the CMIA, Plaintiff and the Class members have suffered (and will continue to suffer) economic damages and other injury and actual harm in the form of, among other things:

a. present, imminent, immediate and continuing increased risk of identity theft, identity fraud and medical fraud –risks justifying expenditures for protective and remedial services for which they are entitled to compensation;

b. invasion of privacy;

c. breach of the confidentiality of their PHI;

d. statutory damages under the CMIA;

e. deprivation of the value of their PHI, for which there is a well-established market; and

f. the financial and temporal cost of monitoring their credit, monitoring their financial accounts, and mitigating their damages.

113. As a direct and proximate result of Defendant's wrongful actions, inaction, omission, and want of ordinary care that directly and proximately caused the release of

Plaintiff's and Class members' PHI, Plaintiff and Class members' personal medical information was viewed by, released to, and disclosed to third parties without Plaintiff's and Class members' written authorization.

114. Defendant's negligent failure to maintain, preserve, store, abandon, destroy, and/or dispose of Plaintiff's and Class members' medical information in a manner that preserved the confidentiality of the information contained therein violated the CMIA.

115. Plaintiff and the Class members were injured and have suffered damages, as described above, from Defendant's illegal and unauthorized disclosure and negligent release of their medical information in violation of Cal. Civ. Code §§56.10 and 56.101, and therefore seek relief under Civ. Code §§ 56.35 and 56.36, which allows for actual damages, nominal statutory damages of $1,000, punitive damages of $3,000, injunctive relief, and attorneys' fees, expenses and costs.

COUNT IV
Violation of California Unfair Competition Law ("UCL")
Cal. Bus. & Prof. Code §§ 17200, et. seq.
(On Behalf of Plaintiff and the California Class)

116. Plaintiff repeats and realleges every allegation set forth in the preceding paragraphs.

117. Plaintiff and Defendant are "persons" as defined by Cal. Bus. & Prof. Code § 17201.

118. The UCL prohibits "unlawful, unfair, or fraudulent business acts or practices."

119. By failing to take reasonable precautions to protect the PII and PHI of Plaintiff and the Class, Defendant has engaged in "unlawful" and "unfair" business practices in violation of the UCL.

120. First, Defendant engaged in "unlawful" acts or practices because it violated multiple laws, including the California Confidentiality of Medical Information Act, Cal. Civ. Code § 56, et seq.; the FTC Act; and the common law, all as alleged herein.

121. Second, Defendant engaged in "unfair" acts or practices, including the following:

a. Defendant failed to implement and maintain reasonable data security measures to protect the Class members' PII and PHI. Defendant failed to identify foreseeable security risks and adequately maintain their data security considering the known risk of cyber intrusions, especially in light of the highly sensitive nature of the information which Defendant stored. Defendant's conduct, with little if any social utility, is unfair when weighed against the harm to the Class members whose PII and PHI has been compromised;

b. Defendant's failure to implement and maintain reasonable data security measures was contrary to legislatively declared public policy that seeks to protect consumers' personal information and ensures that entities entrusted with PII and PHI adopt appropriate security measures. These policies are reflected in various laws, including the FTC Act (15 U.S.C. § 45); and the California Confidentiality of Medical Information Act (Cal. Civ. Code § 56, et seq.); and

c. Defendant's failure to implement and maintain reasonable data security measures led to the substantial consumer injuries described herein. These injuries are not outweighed by countervailing benefits to consumers or competition. Moreover, because consumers could not have reasonably known of Defendant's inadequate

data security, consumers could not have reasonably avoided the harm that Defendant's conduct caused.

122. As a direct and proximate result of Defendant's acts of unlawful and unfair practices and acts, Plaintiff and the Class were injured and lost money or property and suffered the various types of damages alleged herein.

123. The UCL states that an action may be brought by any person who has "suffered injury in fact and has lost money or property as a result of the unfair competition." Cal. Bus. & Prof. Code § 17204. Plaintiff and the Class Members suffered injury in fact and lost money or property, including in the form of the loss of value of their breached PII and PHI, as a result of Defendant's unfair competition as set forth herein. PII and PHI are valuable which is demonstrated by the fact that Defendant's business is built in part by managing the PII and PHI of the Class.

124. Plaintiff and the Class are entitled to injunctive relief to address Defendant's past and future acts of unfair competition.

125. Plaintiff and the Class are entitled to restitution of money and property that Defendant obtained by means of unlawful, unfair, or fraudulent practices, and restitutionary disgorgement of all profits accruing to Defendant as a result of their unlawful and unfair business practices.

126. Plaintiff lacks an adequate remedy at law because the injuries here include an imminent risk of identity theft and fraud that can never be fully remedied through damages.

127. Further, if an injunction is not issued, Plaintiff and Class members will suffer irreparable injury. The risk of another such breach is real, immediate, and substantial. Plaintiff and Class members lack an adequate remedy at law that will reasonably protect them against the

risk of such further breach.

128. Plaintiff and the Class seek all monetary and non-monetary relief available to them under the UCL, including reasonable attorney's fees as allowed under Cal. Code Civ. Proc. §1021.5.

COUNT V
Unjust Enrichment

(On Behalf of Plaintiff and the Nationwide Class or Alternatively State-Specific Subclasses)

129. Plaintiff repeats and realleges every allegation set forth in the preceding paragraphs.

130. Plaintiff and Class members have an interest, both equitable and legal, in the PII and PHI about them that was conferred upon, collected by, and maintained by Defendant and that was ultimately accessed in the Data Breach.

131. Defendant was benefitted by the conferral upon it of the PII and PHI pertaining to Plaintiff and Class members and by its ability to retain, use, and profit from that information. Defendant understood that it was in fact so benefitted.

132. Defendant also understood and appreciated that the PII and PHI pertaining to Plaintiff and Class members was private and confidential and its value depended upon Defendant maintaining the privacy and confidentiality of that PII and PHI.

133. But for Defendant's willingness and commitment to maintain its privacy and confidentiality, that PII and PHI would not have been transferred to and entrusted with Defendant.

134. Defendant continues to benefit and profit from its retention and use of the PII and PHI while its value to Plaintiff and Class members has been diminished.

135. Defendant also benefitted through its unjust conduct by selling its services for more than those services were worth to Plaintiff and Class members, who would not have purchased Apria's products or services had they been aware that Defendant would fail to protect their PII and PHI.

136. Defendant also benefitted through its unjust conduct by retaining money that it should have used to provide reasonable and adequate data security to protect Plaintiff's and Class members' PII and PHI.

137. It is inequitable for Defendant to retain these benefits.

138. As a result of Defendant's wrongful conduct as alleged in this Complaint (including, among things, its knowing failure to employ adequate data security measures, its continued maintenance and use of the PII and PHI belonging to Plaintiff and Class members without having adequate data security measures, and its other conduct facilitating the theft of that PII and PHI), Defendant has been unjustly enriched at the expense of, and to the detriment of, Plaintiff and Class members.

139. Defendant's unjust enrichment is traceable to, and resulted directly and proximately from, the conduct alleged herein, including the compiling and use of Plaintiff's and Class members' PII and PHI, while at the same time failing to maintain that information secure from intrusion and theft by hackers and identity thieves.

140. Under the common law doctrine of unjust enrichment, it is inequitable for Defendant to be permitted to retain the benefits it received, and is still receiving, without justification, from Plaintiff and Class members in an unfair and unconscionable manner. Defendant's retention of such benefits under circumstances making it inequitable to do so constitutes unjust enrichment.

141. The benefits conferred upon, received, and enjoyed by Defendant were not conferred officiously or gratuitously, and it would be inequitable and unjust for Defendant to retain these benefits.

142. Plaintiff and Class members have no adequate remedy at law for Defendant's unjust enrichment.

Defendant is therefore liable to Plaintiff and Class members for restitution or disgorgement in the amount of the benefit conferred on Defendant as a result of its wrongful conduct, including specifically: the value to Defendant of the PII and PHI that was compromised in the Data Breach; the profits Defendant is receiving from the use of that information; the amounts that Defendant overcharged Plaintiff and Class members for its products and use of its services; and the amounts that Defendant should have spent to provide reasonable and adequate data security to protect Plaintiff's and Class members' PII and PHI.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of himself and Class Members, requests judgment against Defendant and that the Court grant the following:

(a) That the Court determine that Plaintiff's claims are suitable for class treatment and certify the proposed Classes pursuant to Fed. R. Civ. P. 23;

(b) That the Court appoint Plaintiff as representative of the Classes;

(c) That Plaintiff's counsel be appointed as counsel for the Classes;

(d) That the Court award compensatory, statutory, and punitive damages;

(e) In the alternative, that the Court award nominal damages as permitted by law;

(f) That the Court award injunctive or other equitable relief that directs Defendant to provide Plaintiff and the Classes with free identity theft protection and credit monitoring,

and to implement reasonable security procedures and practices to protect customers' PII and PHI that conform to relevant federal and state guidelines and industry norms;

(g) That the Court award reasonable costs and expenses incurred in prosecuting this action, including attorneys' fees and expert fees; and

(i) Such other relief as the Court may deem just and proper.

VII. DEMAND FOR JURY TRIAL

Pursuant to Fed. R. Civ. P. 38(b), Plaintiff demands a trial by jury of all issues properly triable to a jury in this case.

Dated: June 21, 2023

By: */s/ M. Anderson Berry*

M. ANDERSON BERRY
aberry@justice4you.com
GREGORY HAROUTUNIAN
gharoutunian@justice4you.com
BRANDON P. JACK
bjack@justice4you.com
CLAYEO C. ARNOLD
A PROFESSIONAL CORPORATION
865 Howe Avenue
Sacramento, CA 95825
Telephone: (916) 239-4778
Fax: (916) 924-1829

Kim D. Stephens, P.S., WSBA #11984*
Kaleigh N. Boyd, WSBA #52684*
TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, WA 98101
Tel: (206) 682-5600/Fax: (206) 682-2992
kstephens@tousley.com
kboyd@tousley.com

** Application for Admission Forthcoming*

Attorneys for Plaintiff and the Proposed Class

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

UNITED STATES DISTRICT COURT

for the

Southern District of Indiana

ANTHONY BOYD, individually, and on behalf of all others similarly situated,

Plaintiff(s)

v.

APRIA HEALTHCARE LLC

Defendant(s)

Civil Action No. 1:23-cv-1085

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-1085

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:

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

ANTHONY BOYD, 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

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. 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 _____ DOCKET NUMBER _____

DATE
06/21/2023

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.