UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF INDIANA
INDIANAPOLIS DIVISION

IN RE APRIA DATA BREACH LITIGATION	Master File No. 1:23-cv-01003-RLY-KMB
This Document Relates To: All Plaintiffs	

CONSOLIDATED CLASS ACTION COMPLAINT

Plaintiffs Lisa Smith, Robert N. Herrera, Suzanne Cuyle, Leonardo DePinto, Joel Kamisher, Debbie Bobbitt, Dottie Nikolich, Sabrina Munoz, Hilary French, Elisa Stroffolino, Amy Clark, Reginald Reese, Rita May, Tammie Creek, Sonya Albert, Paul Kramer, Chad Hohenbery, Colleen Rickard, Kristina Accardo, Roger Winstanley, and Bonnie Bennett ("Plaintiffs"), individually and on behalf of all similarly situated persons, allege the following against Apria Healthcare LLC ("Apria" or "Defendant") based upon personal knowledge with respect to themselves and on information and belief derived from, among other things, investigation by their counsel and review of public documents, as to all other matters:

INTRODUCTION

1. Plaintiffs bring this class action against Apria for its failure to properly secure and safeguard Plaintiffs' and other similarly situated Apria patients' sensitive information, including full names, addresses, financial account information, and contact information ("personally identifiable information" or "PII"), as well as Protected Health Information ("PHI"), including medical information and treatment information (collectively with PII, "Private

Information") from criminal hackers.[1]

2. Apria is a provider of home medical equipment for sleep apnea and other medical conditions, serving medical providers and patients across the country.

3. On or about September 1, 2021, "Apria received a notification regarding access to select Apria systems by an unauthorized third party," and, through its subsequent investigation, determined that a threat actor had access to its systems from April 5, 2019, to May 7, 2019, and again from August 27, 2021, to October 10, 2021 (the "Data Breach").[2]

4. Despite the fact that, under state and federal law, organizations must report breaches that impact PHI within at least 60 days, Apria waited more than eight months after it discovered the initial Data Breach to file official notice of a hacking incident on or around May 22, 2023.

5. On or around May 22, 2023, Apria also posted a Notice of Data Breach to its website, informing its patients of the hacking incident, though not providing sufficient detail regarding its occurrence.

6. At or around that time, Apria also sent Notice of Data Breach letters to approximately 1,869,598 impacted patients, including Plaintiffs and Class Members ("Notice Letter").

7. Thus, Apria waited, in some cases, over ***three years*** from the initial intrusion to disclose the Data Breach to impacted victims.

---

[1] https://www.hipaajournal.com/apria-healthcare-breach-affects-up-to-1-8-million-individuals/ (last visited Oct. 5, 2023); *see also* https://apps.web.maine.gov/online/aeviewer/ME/40/bf218a4e-1ffd-4f14-a74d-3d34aec8d6c7.shtml (noting that, "Financial Account Number or Credit/Debit Card number (in combination with security code, access code, password or PIN for the account" were also impacted) (last visited Oct. 5, 2023).

[2] *See* the "Notice Letter," *available at* https://apps.web.maine.gov/online/aeviewer/ME/40/ bf218a4e-1ffd-4f14-a74d-3d34aec8d6c7.shtml (last visited Oct. 5, 2023).

8. As a result of this delayed response, Plaintiffs and Class Members had no idea for years that their Private Information had been compromised, and that they were, and continue to be, exposed to an ongoing and lifetime risk of identity theft and various other forms of personal, social, and financial harm.

9. The Private Information compromised in the Data Breach contained highly sensitive patient data, representing a goldmine for data thieves. The data included, but is not limited to, full names, addresses, contact information, financial account information, medical information, and treatment information that Apria collected and maintained.

10. Armed with the Private Information accessed in the Data Breach, data thieves can commit a variety of crimes including, *e.g.*, opening new financial accounts in Class Members' names, taking out loans in Class Members' names, using Class Members' names to obtain medical services, using Class Members' information to obtain government benefits, filing fraudulent tax returns using Class Members' information, obtaining driver's licenses in Class Members' names but with another person's photograph, and giving false information to police during an arrest.

11. Apria has offered no assurances that all personal data or copies of data have been recovered or destroyed, or that Apria has adequately enhanced its data security practices sufficient to avoid a similar breach of its network in the future.

12. Therefore, Plaintiffs and Class Members have suffered and are at a present and continuing increased risk of suffering, ascertainable losses in the form of harm from identity theft and other fraudulent misuse of their Private Information, the loss of the benefit of their bargain, out-of-pocket expenses incurred to remedy or mitigate the effects of the Data Breach, and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach.

13. Plaintiffs bring this class action lawsuit to address Apria's inadequate safeguarding of Class Members' Private Information that it collected and maintained, and its failure to provide timely and adequate notice to Plaintiffs and Class Members of the types of information that were accessed, and that such information was subject to unauthorized access by cybercriminals.

14. The potential for improper disclosure and theft of Plaintiffs' and Class Members' Private Information was a known risk to Apria, and thus Apria was on notice that failing to take necessary steps to secure the Private Information left it vulnerable to an attack.

15. Upon information and belief, Apria failed to properly monitor and properly implement security practices with regard to its computer network and systems that housed the Private Information. Had Apria properly monitored its networks, it would have discovered the Data Breach sooner.

16. Plaintiffs' and Class Members' identities are now at risk because of Apria's negligent conduct, as the Private Information that Apria collected and maintained is now in the hands of thieves and other unauthorized third parties.

17. Plaintiffs seek to remedy these harms on behalf of themselves and all similarly situated individuals whose Private Information was accessed and/or compromised during the Data Breach.

PARTIES

18. Plaintiff Lisa Smith is, and at all times mentioned herein was, a resident and citizen of the State of Illinois.

19. Plaintiff Robert N. Herrera is, and at all times mentioned herein was, a resident and citizen of the State of California.

20. Plaintiff Suzanne Cuyle is, and at all times mentioned herein was, a resident and citizen of the State of Washington.

21. Plaintiff Joel Kamisher is, and at all times mentioned herein was, a resident and citizen of the State of California.

22. Plaintiff Leonardo DePinto is, and at all times mentioned herein was, a resident and citizen of the State of New Jersey.

23. Plaintiff Debbie Bobbitt is, and at all times mentioned herein was, a resident and citizen of the State of Illinois.

24. Plaintiff, Dottie Nikolich, is, and at all times mentioned herein was, a resident and citizen of the State of Illinois.

25. Plaintiff, Sabrina Munoz, is, and at all times mentioned herein was, a resident and citizen of the State of New York.

26. Plaintiff, Hilary French, is, and at all times mentioned herein was, a resident and citizen of the State of Colorado.

27. Plaintiff, Elisa Stroffolino, is, and at all times mentioned herein was, a resident and citizen of the State of California.

28. Plaintiff, Amy Clark, is, and at all times mentioned herein was, a resident and citizen of the State of Ohio.

29. Plaintiff, Reginald Reese, is, and at all times mentioned herein was, a resident and citizen of the State of California.

30. Plaintiff, Rita May, is, and at all times mentioned herein was, a resident and citizen of the State of Missouri.

31. Plaintiff, Tammie Creek, is, and at all times mentioned herein was, a resident and

citizen of the State of Arkansas.

32. Plaintiff, Sonya Albert, is, and at all times mentioned herein was, a resident and citizen of the State of Georgia.

33. Plaintiff, Paul Kramer, is, and at all times mentioned herein was, a resident and citizen of the State of California.

34. Plaintiff, Chad Hohenbery, is, and at all times mentioned herein was, a resident and citizen of the State of Illinois.

35. Plaintiff, Colleen Rickard, is, and at all times mentioned herein was, a resident and citizen of the State of Nebraska.

36. Plaintiff, Kristina Accardo, is, and at all times mentioned herein was, a resident and citizen of the State of Wisconsin

37. Plaintiff, Roger Winstanley, is, and at all times mentioned herein was, a resident and citizen of the State of Wisconsin.

38. Plaintiff, Bonnie Bennett, is, and at all times mentioned herein was, a resident and citizen of the State of Missouri.

39. Defendant, Apria Healthcare LLC, is a Delaware limited liability company with its principal place of business located at 7353 Company Drive, Indianapolis, Indiana 46237. The sole member of Apria Healthcare LLC is Apria Healthcare Group LLC, a Delaware limited liability company with its principal place of business in Indianapolis, Indiana. The sole member of Apria Healthcare Group LLC is Apria Holdco LLC, a Delaware limited liability company with its principal place of business in Indianapolis, Indiana. The sole member of Apria Holdco LLC is Apria, Inc., a Delaware corporation with its principal place of business in Indianapolis, Indiana. Defendant is a provider of home medical equipment for sleep apnea and other medical conditions

and serves medical providers and patients across the country.

JURISDICTION AND VENUE

40. The 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. The number of Class Members is over 100, many of whom, including each of the named Plaintiffs, have different citizenship from Apria. Thus, minimal diversity exists under 28 U.S.C. §1332(d)(2)(A).

41. This Court has personal jurisdiction over Apria because it has sufficient minimum contacts in Indiana, including its headquarters and principal place of business, and intentionally avails itself of this jurisdiction by marketing and selling products and services in Indiana.

42. Venue is proper in this District pursuant to 28 U.S.C. § 1391(b) because Apria maintains its corporate offices in this District, and Apria is subject to the Court's personal jurisdiction with respect to this action.

FACTUAL ALLEGATIONS

A. The Data Breach

43. Apria provides home healthcare equipment to nearly 2 million patients across the United States.[3] 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.

44. Apria's patients and customers entrust Apria with their Private Information to obtain Apria's services and do so on the mutual understanding that Apria will implement

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

reasonable data security sufficient to safeguard the Private Information of Plaintiffs and Class Members.

45. Indeed, just three years ago, 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."[4]

46. But while it was holding itself out to the public as a leader in keeping its patients' data private, Apria allowed that data to be accessed by criminal third parties. In May 2023, Apria admitted it was the subject of a massive data breach that affected millions of its patients and customers. Specifically, 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 the Private Information of its customers (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. These cybercriminals went undetected as they accessed this Private Information over the course of several months in 2019 and 2021.

47. The Private Information 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.

48. 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. Apria

[4] *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=1b198c273cb9 (last visited October 22, 2023).

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 Private Information had been compromised.

B. Apria's Business.

49. To obtain healthcare services and products, Apria's customers and patients must provide their highly sensitive Private Information to doctors, medical professionals, insurance companies, or to Apria directly, or sometimes all four. As part of their business, Apria then compiles, stores, and maintains the Private Information it receives from customers, healthcare professionals, and insurers who submit Class Members' Private Information to receive Apria's goods or services.

50. Because of the highly sensitive and personal nature of the information Apria acquires and stores with respect to patients and customers, Apria, upon information and belief, promises to, among other things: keep Private Information private; comply with health care industry standards related to data security and Private Information, including the Health Insurance Portability and Accountability Act of 1996, as amended, and its implementing regulations ("HIPAA"); inform consumers of its legal duties and comply with all federal and state laws protecting consumer Private Information; use and release Private Information only for reasons that relate to medical care and treatment; and provide adequate notice to individuals if their Private Information is disclosed without authorization.

51. By obtaining, collecting, using, and deriving a benefit from Plaintiffs' and Class Members' Private Information, Apria assumed legal and equitable duties to Plaintiffs and Class Members, and it knew or should have known that it was responsible for protecting Plaintiffs' and Class Members' Private Information from unauthorized disclosure.

52. Apria was in the best position to safeguard the most sensitive information that it obtained from Plaintiffs and Class Members. Its unique position enabled it to collect some of the most sensitive information on Plaintiffs and Class Members; accordingly, Apria had a special relationship with Plaintiffs and Class Members such that it should have safeguarded that data.

53. Apria had obligations to Plaintiffs and to Class Members to safeguard their Private Information and to protect it from unauthorized access and disclosure. Indeed, Plaintiffs and Class Members provided their Private Information 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 data breaches of major companies before the Data Breach.

54. Apria also promises to keep its customers' Private Information secure, as it is legally required to do under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA").

55. 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."[5] 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."[6]

56. Had Apria told patients that it would not protect their Private Information, the Plaintiffs would not have provided Apria with their Private Information and would not have sought

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

treatment and services with Apria.

57. Apria failed to uphold these data security and privacy promises and did not maintain adequate or commercially acceptable security to protect its systems from infiltration by cybercriminals, and the Privacy Information of over 1.8 million individuals was compromised as a result. Worse, Apria waited years to publicly disclose the Data Breach.

C. Apria is a Covered Entity Subject to HIPAA.

58. Apria is a HIPAA-covered entity that provides services and products directly to patients. As a regular and necessary part of its business, Apria collects the highly sensitive Private Information of its customers and patients.

59. Defendant is a covered entity pursuant to the Health Insurance Portability and Accountability Act ("HIPAA"). *See* 45 C.F.R. § 160.102. Defendant must therefore comply with the HIPAA Privacy Rule and Security Rule. *See* 45 C.F.R. Part 160 and Part 164, Subparts A through E.

60. Defendant is a covered entities pursuant to the Health Information Technology Act ("HITECH")[7]. *See* 42 U.S.C. §17921, 45 C.F.R. § 160.103.

61. HIPAA's Privacy Rule, otherwise known as "Standards for Privacy of Individually Identifiable Health Information," establishes national standards for the protection of health information.

62. HIPAA's Security Rule, otherwise known as "Security Standards for the Protection of Electronic Protected Health Information," establishes national security standards for the protection of health information that is held or transferred in electronic form. See 42 C.F.R. §§

[7] HIPAA and HITECH work in tandem to provide guidelines and rules for maintaining protected health information. HITECH references and incorporates HIPAA.

164.302-164.318.

63. HIPAA limits the permissible uses of "protected health information" and prohibits the unauthorized disclosure of "protected health information." 45 C.F.R. § 164.502. HIPAA requires that covered entities implement appropriate administrative, technical, and physical safeguards for this information and requires that covered entities reasonably safeguard protected health information from any intentional or unintentional use or disclosure that is in violation of the standards, implementation specifications or other requirements of this subpart. *See* 45 C.F.R. § 164.530(c).

64. HIPAA requires a covered entity to have and apply appropriate sanctions against members of its workforce who fail to comply with the privacy policies and procedures of the covered entity or the requirements of 45 C.F.R. Part 164, Subparts D or E. *See* 45 C.F.R. § 164.530(e).

65. HIPAA requires a covered entity to mitigate, to the extent practicable, any harmful effect that is known to the covered entity of a use or disclosure of protected health information in violation of its policies and procedures or the requirements of 45 C.F.R. Part 164, Subpart E by the covered entity or its business associate. *See* 45 C.F.R. § 164.530(f).

66. Under HIPAA:

> Protected health information means individually identifiable health information:
>
> (1) Except as provided in paragraph (2) of this definition, that is:
>
> (i) Transmitted by electronic media;
>
> (ii) Maintained in electronic media; or
>
> (iii) Transmitted or maintained in any other form or medium.[8]

[8] 45 C.F.R. § 160.103

67. HIPAA and HITECH obligated Defendant to implement technical policies and procedures for electronic information systems that maintain electronic protected health information so that such systems were accessible only to those persons or software programs that had been granted access rights and who have a working need to access and view the information. *See* 45 C.F.R. § 164.312(a)(1); *see also* 42 U.S.C. §17902.

68. HIPAA and HITECH also obligated Defendant to implement policies and procedures to prevent, detect, contain, and correct security violations, and to protect against uses or disclosures of electronic protected health information that are reasonably anticipated but not permitted by the privacy rules. *See* 45 C.F.R. § 164.306(a)(1) and § 164.306(a)(3); *see also* 42 U.S.C. §17902.

69. HIPAA further obligated Defendant to ensure that its workforce complied with HIPAA security standard rules (*see* 45 C.F.R. § 164.306(a)(4)) to effectively train its workforces on the policies and procedures with respect to protected health information, as necessary and appropriate for those individuals to carry out their functions and maintain the security of protected health information. *See* 45 C.F.R. § 164.530(b)(1).

70. HIPAA also requires the Office of Civil Rights ("OCR"), within the Department of Health and Human Services ("HHS"), to issue annual guidance documents on the provisions in the HIPAA Security Rule. *See* 45 C.F.R. §§ 164.302-164.318. For example, "HHS has developed guidance and tools to assist HIPAA covered entities in identifying and implementing the most cost effective and appropriate administrative, physical, and technical safeguards to protect the confidentiality, integrity, and availability of e-PHI and comply with the risk analysis requirements of the Security Rule." *See* US Department of Health & Human Services, Security Rule Guidance

Material.[9] The list of resources includes a link to guidelines set by the National Institute of Standards and Technology (NIST), which OCR says "represents the industry standard for good business practices with respect to standards for securing e-PHI." *See* US Department of Health & Human Services, Guidance on Risk Analysis.[10]

71. Should a health care provider experience an unauthorized disclosure, it is required to conduct a Four Factor Risk Assessment (HIPAA Omnibus Rule). This standard requires, "A covered entity or business associate must now undertake a four-factor risk assessment to determine whether or not PHI has been compromised and overcome the presumption that the breach must be reported. The four-factor risk assessment focuses on:

> (1) the nature and extent of the PHI involved in the incident (e.g., whether the incident involved sensitive information like social security numbers or infectious disease test results);
>
> (2) the recipient of the PHI;
>
> (3) whether the PHI was actually acquired or viewed; and
>
> (4) the extent to which the risk that the PHI was compromised has been mitigated following unauthorized disclosure (e.g., whether it was immediately sequestered and destroyed)."[11]

72. The HIPAA Breach Notification Rule, 45 CFR §§ 164.400-414, requires HIPAA covered entities and their business associates to provide notification following a breach of unsecured protected health information.

---

[9] http://www.hhs.gov/hipaa/for-professionals/security/guidance/index.html
[10]https://www.hhs.gov/hipaa/for-professionals/security/guidance/guidance-risk-analysis/index.html
[11] 78 Fed. Reg. 5641-46, *See also*, 45 C.F.R. §164.304

73. The HIPAA Contingency Operations Rule, 45 C.F.R. §164.301(a), requires a healthcare provider to have security measures in place and train its employees and staff so that all its staff and employees know their rolls in facility security.

74. Defendant failed to provide proper notice to Plaintiff of the disclosure.

75. Defendant failed to conduct or improperly conducted the four-factor risk assessment following the unauthorized disclosure.

76. As a direct and/or proximate result of Defendant's wrongful actions and/or inaction and the resulting Breach, the criminal(s) and/or their customers now have Plaintiff's and the other Class Members' compromised PHI and PII.

77. Due to the nature of Apria's business, which includes providing a range of healthcare services, including storing and maintaining electronic health records, Apria would be unable to engage in its regular business activities without collecting and aggregating Private Information that it knows and understands to be sensitive and confidential.

78. Plaintiffs and Class Members are or were customers or patients whose Private Information, including medical records, Apria maintained, who received health-related or other services from Apria, and/or individuals who directly or indirectly entrusted Apria with their Private Information.

79. Plaintiffs and Class Members relied on Apria to implement and follow adequate data security policies and protocols, to keep their Private Information confidential and securely maintained, to use such Private Information solely for business and health care purposes, and to prevent the unauthorized disclosures of their Private Information. Plaintiffs and Class Members reasonably expected that Apria would safeguard their highly sensitive information and keep that Private Information confidential.

80. As described throughout this Complaint, Apria did not reasonably protect, secure, or store Plaintiffs' and Class Members' Private Information prior to, during, or after the Data Breach, but rather, enacted unreasonable data security measures that it knew or should have known were insufficient to reasonably protect the highly sensitive information Apria maintained. Predictably, cybercriminals circumvented Apria's security measures, resulting in a significant Data Breach.

D. A Data Breach Was a Foreseeable Risk of which Apria Was on Notice.

81. As a HIPAA-covered business entity that collects, creates, and maintains significant volumes of Private Information, Apria was aware that a targeted attack was a foreseeable risk that it had a duty to guard against. It is well-known that healthcare businesses such as Apria, which collects and stores the confidential and sensitive Private Information of millions of individuals, are frequently targeted by cyberattacks. Further, cyberattacks are highly preventable through the implementation of reasonable and adequate cybersecurity safeguards, including proper employee cybersecurity training.

82. Apria's data security obligations were particularly important given the substantial increase in cyberattacks and/or data breaches in the healthcare industry, and other industries holding significant amounts of Private Information before the Data Breach.

83. The targeted cyberattack was expressly designed to gain access to and exfiltrate private and confidential data, including (among other things) the Private Information of patients and customers, like Plaintiffs and Class Members.

84. Apria was on notice that such an attack was coming: At all relevant times, Apria knew, or should have known, that Plaintiffs' and Class Members' Private Information was a target for malicious actors. Despite such knowledge, Apria failed to implement and maintain reasonable

and appropriate data privacy and security measures to protect Plaintiffs' and Class Members' Private Information from cyberattacks.

85. Moreover, Apria failed to implement and maintain reasonable and appropriate data privacy and security measures that would timely alert Apria of any such attack, should one occur. In the present case, Apria failed to discover the Data Breach for years following the initial attack.

86. Considering recent high profile data breaches at other health care providers, Apria knew or should have known that its electronic records and consumers' Private Information would be targeted by cybercriminals and ransomware attack groups.

87. In particular, cybercriminals seek out PHI at a greater rate than other sources of personal information. In a 2022 report, the healthcare compliance company, Protenus, found that there were 905 medical data breaches in 2021, leaving over 50 million patient records exposed for 700 of the 2021 incidents. This is an increase from the 758 medical data breaches that Protenus compiled in 2020.[12]

88. The healthcare sector suffered about 337 breaches in the first half of 2022 alone, according to Fortified Health Security's mid-year report released in July. The percentage of healthcare breaches attributed to malicious activity rose more than five percentage points in the first six months of 2022 to account for nearly 80 percent of all reported incidents.[13]

89. In light of recent high profile cybersecurity incidents at other healthcare partner and provider companies, including American Medical Collection Agency (25 million patients,

[12] *2022 Breach Barometer*, PROTENUS, https://blog.protenus.com/key-takeaways-from-the-2022-breach-barometer (2022).

[13] Jill McKeon, *Health Sector Suffered 337 Healthcare Data Breaches in First Half of Year*, Cybersecurity News (July 19, 2022), *available at* https://healthitsecurity.com/news/health-sector-suffered-337-healthcare-data-breaches-in-first-half-of-year.

March 2019), University of Washington Medicine (974,000 patients, December 2018), Florida Orthopedic Institute (640,000 patients, July 2020), Wolverine Solutions Group (600,000 patients, September 2018), Oregon Department of Human Services (645,000 patients, March 2019), Elite Emergency Physicians (550,000 patients, June 2020), Magellan Health (365,000 patients, April 2020), BJC Health System (286,876 patients, March 2020), and Premera Blue Cross (10.4 million patients, January 2015). Apria knew or should have known that its electronic records would be targeted by cybercriminals.

90. Indeed, cyberattacks against the healthcare industry have been common for over twelve years, with the FBI warning as early as 2011 that cybercriminals were "advancing their abilities to attack a system remotely" and "[o]nce a system is compromised, cyber criminals will use their accesses to obtain PII." The FBI further warned that that "the increasing sophistication of cyber criminals will no doubt lead to an escalation in cybercrime."[14]

91. PHI is particularly valuable and has been referred to as a "treasure trove for criminals."[15] A cybercriminal who steals a person's PHI can end up with as many as "seven to 10 personal identifying characteristics of an individual."[16] A study by Experian found that the "average total cost" of medical identity theft is "about $20,000" per incident in 2010, and that a majority of victims of medical identity theft were forced to pay out-of-pocket costs for healthcare they did not receive in order to restore coverage.[17]

---

[14] Gordon M. Snow, *Statement before the House Financial Services Committee, Subcommittee on Financial Institutions and Consumer Credit*, FBI (Sept. 14, 2011), https://archives.fbi.gov/archives/news/testimony/cyber-security-threats-to-the-financial-sector.

[15] *See* Andrew Steger, *What Happens to Stolen Healthcare Data?*, HEALTHTECH MAGAZINE (Oct. 30, 2019), https://healthtechmagazine.net/article/2019/10/what-happens-stolen-healthcare-data-perfcon (stating "Health information is a treasure trove for criminals.").

[16] *Id.*

[17] Elinor Mills, *Study: Medical identity theft is costly for victims*, CNET (Mar. 3, 2010), https://www.cnet.com/news/privacy/study-medical-identity-theft-is-costly-for-victims/.

92. Cyberattacks on medical systems, like Apria's, have become so notorious that the 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 and hospitals are attractive . . . because they often have lesser IT defenses and a high incentive to regain access to their data quickly."[18]

93. According to an article in the HIPAA Journal posted on October 14, 2022, cybercriminals hack into medical practices for their "highly prized" medical records. "[T]he number of data breaches reported by HIPAA-regulated entities continues to increase every year. 2021 saw 714 data breaches of 500 or more records reported to the [HHS' Office for Civil Rights] OCR – an 11% increase from the previous year. Almost three-quarters of those breaches were classified as hacking/IT incidents." [19]

94. Healthcare organizations are easy targets because "even relatively small healthcare providers may store the records of hundreds of thousands of patients. The stored data is highly detailed, including demographic data, Social Security numbers, financial information, health insurance information, and medical and clinical data, and that information can be easily monetized."[20] In this case, Apria stored the records of *millions* of patients and consumers.

95. Private Information, like that stolen from Apria, is "often processed and packaged with other illegally obtained data to create full record sets (Fullz) that contain extensive information on individuals, often in intimate detail." The record sets are then sold on dark web sites to other criminals and "allows an identity kit to be created, which can then be sold for

---

[18] *FBI, Secret Service Warn of Targeted*, Law360 (Nov. 18, 2019), https://www.law360.com/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware.

[19] The HIPAA Journal, *Editorial: Why Do Criminals Target Medical Records* (Oct. 14, 2022), https://www.hipaajournal.com/why-do-criminals-target-medical-records.

[20] *See id.*

considerable profit to identity thieves or other criminals to support an extensive range of criminal activities."[21]

96. Cybercriminals also maintain encrypted information on individuals to sell in "Fullz" records because that information can be foreseeably decrypted in the future.

97. Apria was on notice that the FBI has recently been concerned about data security in the healthcare industry. In August 2014, after a cyberattack on Community Health Systems, Inc., the FBI warned companies within the healthcare industry that hackers were targeting them. The warning stated that "[t]he FBI has observed malicious actors targeting healthcare related systems, perhaps for the purpose of obtaining the Protected Healthcare Information (PHI) and/or Personally Identifiable Information (PII)."[22]

98. The American Medical Association ("AMA") has also warned healthcare companies about the importance of protecting their patients' confidential information:

> Cybersecurity is not just a technical issue; it's a patient safety issue. AMA research has revealed that 83% of physicians work in a practice that has experienced some kind of cyberattack. Unfortunately, practices are learning that cyberattacks not only threaten the privacy and security of patients' health and financial information, but also patient access to care.[23]

99. As implied by the above AMA quote, stolen Private Information can be used to interrupt important medical services. This is an imminent and certainly impending risk for Plaintiffs and Class Members.

100. The U.S. Department of Health and Human Services and the Office of Consumer

---

[21] *See id*.

[22] Jim Finkle, *FBI Warns Healthcare Firms that they are Targeted by Hackers*, REUTERS (Aug. 2014), https://www.reuters.com/article/us-cybersecurity-healthcare-fbi/fbi-warns-healthcare-firms-they-are-targeted-by-hackers-idINKBN0GK24U20140820.

[23] Andis Robeznieks, *Cybersecurity: Ransomware attacks shut down clinics, hospitals*, AM. MED. ASS'N (Oct 4, 2019), https://www.ama-assn.org/practice-anagement/sustainability/cybersecurity-ransomware-attacks-shut-down-clinics-hospitals.

Rights urges the use of encryption of data containing sensitive personal information. As far back as 2014, the Department fined two healthcare companies approximately two million dollars for failing to encrypt laptops containing sensitive personal information. In announcing the fines, Susan McAndrew, formerly OCR's deputy director of health information privacy, stated that "[o]ur message to these organizations is simple: encryption is your best defense against these incidents."24

101. As a HIPAA-covered entity, Apria should have known about its data security vulnerabilities and implemented enhanced and adequate protection, particularly given the nature of the Private Information stored in its unprotected files.

E. Apria Failed to Comply with FTC Guidelines.

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

103. 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 Private Information by companies like Apria. 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.

104. 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;

[24] Susan D. Hall, *OCR levies $2 million in HIPAA fines for stolen laptops*, FIERCE HEALTHCARE (Apr. 23, 2014), https://www.fiercehealthcare.com/it/ocr-levies-2-million-hipaa-fines-for-stolen-laptops.

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.

105. 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.

106. 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.

107. 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.[25]

108. Apria was aware or should have been aware of its obligations to protect its

[25] *Privacy and Security Enforcement*, FED. TRADE COMM'N, https://www.ftc.gov/news-events/topics/protecting-consumer-privacy-security/privacy-security-enforcement.

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.

F. Data Breaches Cause Disruption and Put Victims at an Increased Risk of Fraud and Identity Theft.

109. Cyberattacks and data breaches at health care companies like Apria are especially problematic because they can negatively impact the overall daily lives of individuals affected by the attack.

110. Researchers have found that among medical service providers that experience a data security incident, the death rate among patients increased in the months and years after the attack.[26]

111. Researchers have further found that at medical service providers that experienced a data security incident, the incident was associated with deterioration in timeliness and patient outcomes, generally.[27]

112. The United States Government Accountability Office released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft face "substantial costs and time to repair the damage to their good name and credit record."[28]

113. That is because any victim of a data breach is exposed to serious ramifications

---

[26] *See* Nsikan Akpan, *Ransomware and Data Breaches Linked to Uptick in Fatal Heart Attacks*, PBS (Oct. 24, 2019), https://www.pbs.org/newshour/science/ransomware-and-other-data-breaches-linked-to-uptick-in-fatal-heart-attacks.

[27] *See* Sung J. Choi, et al., *Data Breach Remediation Efforts and Their Implications for Hospital Quality*, 54 Health Services Research 971, 971-980 (2019), *available at* https://onlinelibrary.wiley.com/doi/full/10.1111/1475-6773.13203.

[28] *See* U.S. Gov. Accounting Office, GAO-07-737, Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown (June 2007), *available at* https://www.gao.gov/new.items/d07737.pdf.

regardless of the nature of the data. Indeed, the reason criminals steal Private Information is to monetize it. They do this by selling the spoils of their cyberattacks on the black market to identity thieves who desire to extort and harass victims and to take over victims' identities to engage in illegal financial transactions under the victims' names. Because a person's identity is akin to a puzzle, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity, or otherwise harass or track the victim. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails.

114. The FTC recommends that identity theft victims take several steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for seven years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[29]

115. Identity thieves use stolen Private Information such as Social Security numbers for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.

116. Identity thieves can also use Social Security numbers to obtain a driver's license

[29] *See IdentityTheft.gov*, FED. TRADE COMM'N, https://www.identitytheft.gov/Steps (last visited May 7, 2023).

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

117. Moreover, theft of Private Information is also gravely serious because Private Information is an extremely valuable property right.[30]

118. Its value is axiomatic, considering the value of "big data" in corporate America and the fact that 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.

119. An active and robust legitimate marketplace for Private Information exists. In 2019, the data brokering industry was worth roughly $200 billion.[31]

120. In fact, the data marketplace is so sophisticated that consumers can actually sell their non-public information directly to a data broker who in turn aggregates the information and provides it to marketers or app developers.[32,33]

121. Consumers who agree to provide their web browsing history to the Nielsen

[30] *See, e.g.*, John T. Soma, et al., *Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets*, 15 Rich. J.L. & Tech. 11, at *3–4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).
[31] https://www.latimes.com/business/story/2019-11-05/column-data-brokers.
[32] https://datacoup.com/.
[33] https://digi.me/what-is-digime/.

Corporation can receive up to $50.00 a year.[34]

122. Conversely sensitive Private Information can sell for as much as $363 per record on the dark web according to the Infosec Institute.[35]

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

124. In addition, there may be a substantial time lag—measured in years—between when harm occurs and when it is discovered, and also between when Private Information and/or financial information is stolen and when it is used.

125. 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.

See GAO Report, at 29.

126. Private Information is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black-

---

[34] Nielsen Computer & Mobile Panel, *Frequently Asked Questions, available at* https://computermobilepanel.nielsen.com/ui/US/en/faqen.html

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

market" for years.

127. There is a strong probability that entire batches of stolen information have been dumped on the black market and are yet to be dumped on the black market, meaning Plaintiffs and Class Members are at an increased risk of fraud and identity theft for many years into the future.

128. Thus, Plaintiffs and Class Members must vigilantly monitor their financial and medical accounts for many years to come—as Apria has suggested that they do.

129. Private Information can sell for as much as $363 per record according to the Infosec Institute.[36] Private Information is particularly valuable because criminals can use it to target victims with frauds and scams. Once Private Information is stolen, fraudulent use of that information (and the resulting damage to victims) may continue for years.

130. For example, the Social Security Administration has warned that identity thieves can use an individual's Social Security number to apply for additional credit lines.[37] Such fraud may go undetected until debt collection calls commence months, or even years, later. Stolen Social Security numbers also make it possible for thieves to file fraudulent tax returns, file for unemployment benefits, or apply for a job using a false identity.[38] Each of these fraudulent activities is difficult to detect. An individual may not know that his or her Social Security number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

131. Moreover, it is not an easy task to change or cancel a stolen Social Security

[36] *See* Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, InfoSec (July 27, 2015), https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market.
[37] *Identity Theft and Your Social Security Number*, Social Security Administration (July 2021), *available at* https://www.ssa.gov/pubs/EN-05-10064.pdf.
[38] *Id*.

number.

132. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. Even then, a new Social Security number may not be effective, as "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[39]

133. This data, as one would expect, demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "[c]ompared to credit card information, personally identifiable information and Social Security Numbers are worth more than 10x on the black market."[40]

134. Medical information is especially valuable to identity thieves.

135. Theft of PHI, in particular, is gravely serious: "[a] thief may use your name or health insurance numbers to see a doctor, get prescription drugs, file claims with your insurance provider, or get other care. If the thief's health information is mixed with yours, your treatment, insurance and payment records, and credit report may be affected."[41]

136. Because of the value of its collected and stored data, the medical industry has experienced disproportionally higher numbers of data theft events than other industries.

137. For this reason, Apria knew or should have known about these dangers and

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

[40] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, Computer World (Feb. 6, 2015), http://www.itworld.com/article/2880960/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html.

[41] *See Medical Identity Theft*, FED. TRADE COMM'N, http://www.consumer.ftc.gov/articles/0171-medical-identity-theft.

strengthened its data handling systems accordingly. Apria was on notice of the substantial and foreseeable risk of harm from a data breach, yet Apria failed to properly prepare for that risk.

G. The Data Breach Harmed Plaintiffs and Class Members

138. Plaintiffs and Class Members have suffered and will continue to suffer harm because of the Data Breach.

139. Apria recognizes as much and in the Notice Letters it sent to Plaintiffs and Class Members it admonishes them to "remain vigilant by reviewing account statements and monitoring your credit report for unauthorized activity, especially activity that may indicate fraud and identity theft." The Notice Letter further advises Plaintiffs and Class Members to "review recommendations by the Federal Trade Commission regarding identity theft protection" and other "additional steps you can take to help protect yourself."[42] As detailed herein, Plaintiffs followed these recommendations and spent time reviewing their credit reports, changing passwords, contacting their financial institutions, and other reasonable efforts to protect themselves from the present and continuing threat of identity theft and fraud.

140. Plaintiffs 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 Private Information—thereby risking prosecution by listing it for sale on the dark web—if the Private Information was not valuable to malicious actors.

141. The dark web helps ensure users' privacy by effectively hiding server or IP details

[42] Notice Letter, *available at* https://apps.web.maine.gov/online/aeviewer/ME/40/bf218a4e-1ffd-4f14-a74d-3d34aec8d6c7.shtml

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.

142. Malicious actors use Private Information 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.

143. 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.

144. Apria issued misleading public statements about the Data Breach, including its data breach notification letters,[43] in which it attempts to downplay the seriousness of the Data Breach by stating that hackers were likely targeting 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."

145. Apria's intentionally misleading public statements ignore the serious harm its security flaws caused to the Class and conflict with the statements it made in its letter regarding the data breach to Plaintiffs and Class Members. Worse, those statements could convince Class Members that they do not need to take steps to protect themselves.

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

146. The data security community agrees that the Private Information compromised in the Data Breach greatly increases Class Members' risk of identity theft and fraud.

147. 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.[44]

148. Criminals can use the Private Information that Apria failed to protect 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.[45]

149. Criminals can also use the Private Information that Apria failed to protect to commit medical identity theft.[46] 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 Plaintiffs or Class Members' ability to access their own medical care or health insurance benefits, not to mention their credit.

150. The Private Information 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.

151. Malicious actors can use Class Members' Private Information 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

[44] https://www.cnet.com/tech/services-and-software/t-mobile-gets-hacked-again-is-the-un-carrier-un-safe/.
[45] https://consumer.ftc.gov/features/imposter-scams.
[46] https://consumer.ftc.gov/articles/what-know-about-medical-identity-theft.

"synthetic identities."

152. As established above, the Private Information 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 Private Information. Apria states that its mission is to "Improv[e] the Quality of Life for Our Patients at Home."[47] Customers expect that the payments they make to Apria incorporate the costs to implement reasonable security measures to protect patients' and customers' Private Information as part of improving their "quality of life."

153. 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."[48] American companies are estimated to have spent over $19 billion on acquiring personal data of consumers in 2018.[49] It is so valuable to identity thieves that once Private Information has been disclosed, criminals often trade it on the "cyber black-market" or the "dark web" for many years.

154. As a result of their real and significant value, identity thieves and other cyber

[47] https://www.apria.com/about-us.

[48] 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.

[49] 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/.

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.

155. The Private Information accessed in the Data Breach is also very valuable to Plaintiffs 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 addresses for special discounts (*e.g.*, sign-up coupons exchanged for email addresses). Consumers use their unique and valuable Private Information to access the financial sector, including when obtaining a mortgage, credit card, or business loan. As a result of the Data Breach, Plaintiffs and Class Members' Private Information has been compromised and lost significant value.

156. 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."[50]

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

[50] 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.

158. Plaintiffs 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 Private Information 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. Plaintiffs and Class Members will therefore need to continuously monitor their accounts for years to ensure their Private Information obtained in the Data Breach is not used to harm them.

159. 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.

160. 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).

161. 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."

162. Plaintiffs and Class Members 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.

H. Defendant Failed to Take Reasonable Steps to Protect Plaintiffs' and Class Members' Private Information.

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

164. 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.

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

166. Apria could have prevented this Data Breach by properly securing and encrypting the systems containing the Private Information of Plaintiffs and Class Members. Alternatively, Apria 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.

167. Apria's negligence in safeguarding the Private Information of Plaintiffs and Class Members is exacerbated by the repeated warnings and alerts directed to companies like Apria to protect and secure sensitive data they possess.

168. 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.

169. 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.

170. 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.

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

172. Upon information and belief, Apria 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.

173. The Data Breach was a reasonably foreseeable consequence of Apria'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' Private Information.

174. Apria's failure to implement reasonable security systems has caused Plaintiffs and Class Members to suffer and continue to suffer harm that adversely impact Plaintiffs and Class Members economically, emotionally, and/or socially. As discussed above, Plaintiffs 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.

175. In sum, Plaintiffs and Class Members were injured as follows: (i) theft of their Private Information and the resulting loss of privacy rights in that information; (ii) improper disclosure of their Private Information; (iii) the lost value of unauthorized access to their Private Information; (iv) diminution in value of their Private Information; (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 Plaintiffs and Class Members reasonably believed a portion of the sale price would fund reasonable security measures that would protect their Private Information, which was not the case; and/or (viii) nominal damages.

176. Even though Apria offered a year of temporary, non-automatic credit monitoring

to its affected customers, this is insufficient to protect Plaintiffs and Class Members. As discussed above, the threat of identity theft and fraud from the Data Breach will extend for many years and cost Plaintiffs and Class Members significant time and effort.

177. Plaintiffs 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.

PLAINTIFFS' EXPERIENCES

Plaintiff Lisa Smith's Experience

178. Plaintiff Smith provided her Private Information to Defendant as a condition of obtaining a breathing machine from Defendant, which was then entered into Defendant's computer system and maintained by Defendant.

179. Plaintiff Smith reasonably understood and expected that Defendant would safeguard her Private Information and timely and adequately notify her in the event of a data breach. Plaintiff Smith would not have allowed Defendant, or anyone in Defendant's position, to maintain her Private Information if she believed that Defendant would fail to implement reasonable and industry standard practices to safeguard that information from unauthorized access.

180. Plaintiff Smith received a Notice letter from Defendant informing her that her Private Information had been compromised in the Data Breach.

181. Recognizing the present, immediate, and substantially increased risk of harm Plaintiff Smith faces, Defendant offered her a twelve-month subscription to a credit monitoring

service. The Notice letter Plaintiff Smith received also cautioned her to "remain vigilant by reviewing account statements and monitoring your credit report for unauthorized activity, especially activity that may indicate fraud and identity theft."

182. Plaintiff Smith greatly values her privacy and Private Information and takes reasonable steps to maintain the confidentiality of her Private Information. Plaintiff Smith is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

183. Plaintiff Smith stores any and all documents containing Private Information in a secure location and destroys any documents she receives in the mail that contain any Private Information or that may contain any information that could otherwise be used to compromise her identity and credit card accounts. Moreover, she diligently chooses unique usernames and passwords for her various online accounts.

184. As a result of the Data Breach, Plaintiff Smith has spent significant time on activities in response to the Data Breach, including placing "freezes" and "alerts" with credit reporting agencies; contacting her financial institutions; closing or modifying financial accounts; and closely reviewing and monitoring bank accounts, credit reports, insurance statements for unauthorized activity for years to come; and other necessary mitigation efforts. This is valuable time that Plaintiff spent at Defendant's direction and that she otherwise would have spent on other activities, including but not limited to work and/or recreation.

185. The Data Breach has caused Plaintiff Smith to suffer fear, anxiety, and stress, which has been compounded by Defendant's eighteen-month delay in noticing her of the fact that her Social Security number in conjunction with her date of birth were acquired by criminals as a result of the Data Breach.

186. Plaintiff Smith anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. In addition, Plaintiff Smith will continue to be at present and continued increased risk of identity theft and fraud for years to come.

187. Plaintiff Smith has a continuing interest in ensuring that her Private Information, which upon information and belief, remains in Defendant's possession, is protected and safeguarded from future breaches.

Plaintiff Robert N. Herrera's Experience

188. Plaintiff Robert N. Herrera provided his Private Information to Defendant as a condition of receiving healthcare services from Defendant which was then entered into Defendant's computer system and maintained by Defendant.

189. Plaintiff Herrera reasonably understood and expected that Defendant would safeguard his Private Information and timely and adequately notify him in the event of a data breach. Plaintiff Herrera would not have allowed Defendant, or anyone in Defendant's position, to maintain his Private Information if he believed that Defendant would fail to implement reasonable and industry standard practices to safeguard that information from unauthorized access.

190. Plaintiff Herrera received a Notice letter, dated June 6, 2023, from Defendant, informing him that his Private Information had been compromised in the Data Breach. The Notice letter stated that Plaintiff Herrera's name, date of birth, medical device descriptions, patient account number, address, dates of service, email, and telephone number was accessed in the Data Breach.

191. Recognizing the present, immediate, and substantially increased risk of harm

Plaintiff Herrera faces, Defendant offered him a twelve-month subscription to a credit monitoring service. The Notice letter Plaintiff Herrera received also cautioned him to "remain vigilant by reviewing account statements and monitoring your credit report for unauthorized activity, especially activity that may indicate fraud and identity theft."

192. Plaintiff Herrera greatly values his privacy and Private Information and takes reasonable steps to maintain the confidentiality of his Private Information. Plaintiff Herrera is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

193. Plaintiff Herrera stores any and all documents containing Private Information in a secure location and destroys any documents he receives in the mail that contain any Private Information or that may contain any information that could otherwise be used to compromise his identity and credit card accounts. Moreover, he diligently chooses unique usernames and passwords for his various online accounts.

194. To Plaintiff Herrera's knowledge, his PII has not been compromised in a prior data breach.

195. As a result of the Data Breach, Plaintiff Herrera has spent approximately two to four hours researching the Data Breach, verifying the legitimacy of the Notice letter, signing up reviewing his bank accounts, monitoring his credit report, and other necessary mitigation efforts. This is valuable time that Plaintiff spent at Defendant's direction and that he otherwise would have spent on other activities, including but not limited to work and/or recreation.

196. The Data Breach has caused Plaintiff Herrera to suffer fear, anxiety, and stress, which has been compounded by Defendant's eighteen-month delay in noticing him of the fact that his medical information in conjunction with his date of birth was acquired by criminals as a

result of the Data Breach.

197. Plaintiff Herrera anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. In addition, Plaintiff Herrera will continue to be at present and continued increased risk of identity theft and fraud for years to come.

198. Plaintiff Herrera has a continuing interest in ensuring that his Private Information, which upon information and belief, remains in Defendant's possession, is protected and safeguarded from future breaches.

Plaintiff Suzanne Cuyle's Experience

199. Plaintiff Suzanne Cuyle provided her Private Information to Defendant as a condition of receiving healthcare services from Defendant which was then entered into Defendant's computer system and maintained by Defendant.

200. Plaintiff Cuyle reasonably understood and expected that Defendant would safeguard her Private Information and timely and adequately notify her in the event of a data breach. Plaintiff Cuyle would not have allowed Defendant, or anyone in Defendant's position, to maintain her Private Information if she believed that Defendant would fail to implement reasonable and industry standard practices to safeguard that information from unauthorized access.

201. Plaintiff Cuyle received a Notice letter dated June 6, 2023 from Defendant informing her that her Private Information had been compromised in the Data Breach. The Notice letter stated that Plaintiff Cuyle's patient account number, patient email address, and patient name may have been accessed in the Data Breach.

202. Recognizing the present, immediate, and substantially increased risk of harm

Plaintiff Cuyle faces, Defendant offered her a twelve-month subscription to a credit monitoring service. The Notice letter Plaintiff Cuyle received also cautioned her to "remain vigilant by reviewing account statements and monitoring your credit report for unauthorized activity, especially activity that may indicate fraud and identity theft."

203. Plaintiff Cuyle greatly values her privacy and Private Information and takes reasonable steps to maintain the confidentiality of her Private Information. Plaintiff Cuyle is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

204. Plaintiff Cuyle stores any and all documents containing Private Information in a secure location and destroys any documents she receives in the mail that contain any Private Information or that may contain any information that could otherwise be used to compromise her identity and credit card accounts. Moreover, she diligently chooses unique usernames and passwords for her various online accounts.

205. To Plaintiff Cuyle's knowledge, her PII has not been compromised in a prior data breach.

206. As a result of the Data Breach, Plaintiff Cuyle has spent approximately 2 hours on activities to mitigate the harms resulting from the Data Breach including, but not limited to: researching the Data Breach, monitoring her credit report, and other necessary mitigation efforts. This is valuable time that Plaintiff spent at Defendant's direction and that she otherwise would have spent on other activities, including but not limited to work and/or recreation.

207. The Data Breach has caused Plaintiff Cuyle to suffer fear, anxiety, and stress, which has been compounded by Defendant's eighteen-month delay in noticing her of the fact that her PII may have been acquired by criminals as a result of the Data Breach.

208. Plaintiff Cuyle anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. In addition, Plaintiff Cuyle will continue to be at present and continued increased risk of identity theft and fraud for years to come.

209. Plaintiff Cuyle has a continuing interest in ensuring that her Private Information, which upon information and belief, remains in Defendant's possession, is protected and safeguarded from future breaches.

Plaintiff Joel Kamisher's Experience

210. Plaintiff Kamisher provided his Private Information to Defendant as a condition of receiving healthcare products from Defendant, which was then entered into Defendant's computer system and maintained by Defendant.

211. Plaintiff Kamisher reasonably understood and expected that Defendant would safeguard his Private Information and timely and adequately notify him in the event of a data breach. Plaintiff Kamisher would not have allowed Defendant, or anyone in Defendant's position, to maintain his Private Information if he believed that Defendant would fail to implement reasonable and industry standard practices to safeguard that information from unauthorized access.

212. Plaintiff Kamisher received a Notice letter, dated June 6, 2023, from Defendant, informing him that his Private Information had been compromised in the Data Breach. The Notice letter stated that Plaintiff Kamisher's name, patient account number, and patient email address were accessed in the Data Breach.

213. Recognizing the present, immediate, and substantially increased risk of harm Plaintiff Kamisher faces, Defendant offered him a twelve-month subscription to a credit

monitoring service. The Notice letter Plaintiff Kamisher received also cautioned him to "remain vigilant by reviewing account statements and monitoring your credit report for unauthorized activity, especially activity that may indicate fraud and identity theft."

214. Plaintiff Kamisher greatly values his privacy and Private Information and takes reasonable steps to maintain the confidentiality of his Private Information. Plaintiff Kamisher is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

215. Plaintiff Kamisher stores any and all documents containing Private Information in a secure location and destroys any documents he receives in the mail that contain any Private Information or that may contain any information that could otherwise be used to compromise his identity and credit card accounts. Moreover, he diligently chooses unique usernames and passwords for his various online accounts.

216. As a result of the Data Breach, Plaintiff Kamisher has spent significant time on mitigation activities in response to the breach including, researching the Data Breach, verifying the legitimacy of the Notice letter, reviewing his bank accounts, and engaging in other necessary mitigation efforts. This is valuable time that Plaintiff spent at Defendant's direction and that he otherwise would have spent on other activities, including but not limited to work and/or recreation.

217. The Data Breach has caused Plaintiff Kamisher to suffer fear, anxiety, and stress, which has been compounded by Defendant's eighteen-month delay in noticing him of the fact that his Private Information was acquired by criminals as a result of the Data Breach.

218. Plaintiff Kamisher anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. In addition,

Plaintiff Kamisher will continue to be at present and continued increased risk of identity theft and fraud for years to come.

219. Plaintiff Kamisher has a continuing interest in ensuring that his Private Information, which upon information and belief, remains in Defendant's possession, is protected and safeguarded from future breaches.

Plaintiff Leonardo DePinto's Experience

220. Plaintiff DePinto provided his Private Information to Defendant as a condition of receiving products and/or services from Defendant which was then entered into Defendant's computer system and maintained by Defendant.

221. Plaintiff DePinto reasonably understood and expected that Defendant would safeguard his Private Information and timely and adequately notify him in the event of a data breach. Plaintiff DePinto would not have allowed Defendant, or anyone in Defendant's position, to maintain his Private Information if he believed that Defendant would fail to implement reasonable and industry standard practices to safeguard that information from unauthorized access.

222. Plaintiff DePinto received a Notice letter, dated June 6, 2023, from Defendant, informing him that his Private Information had been compromised in the Data Breach. The Notice letter stated that Plaintiff DePinto's name, address, contact information, medical information, and treatment information were accessed by a criminal group.

223. Recognizing the present, immediate, and substantially increased risk of harm Plaintiff DePinto faces, Defendant offered him a twelve-month subscription to a credit monitoring service. The Notice letter Plaintiff DePinto received also cautioned him to "remain vigilant by reviewing account statements and monitoring your credit report for unauthorized

activity, especially activity that may indicate fraud and identity theft."

224. Plaintiff DePinto greatly values his privacy and Private Information and takes reasonable steps to maintain the confidentiality of his Private Information. Plaintiff DePinto is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

225. Plaintiff DePinto stores any and all documents containing Private Information in a secure location and destroys any documents he receives in the mail that contain any Private Information or that may contain any information that could otherwise be used to compromise his identity and credit card accounts. Moreover, he diligently chooses unique usernames and passwords for his various online accounts.

226. As a result of the Data Breach, Plaintiff DePinto has spent significant time on activities in response to the Data Breach, including researching and verifying the legitimacy of the Data Breach upon receiving the Notice Letter and other necessary mitigation efforts. This is valuable time that Plaintiff spent at Defendant's direction and that he otherwise would have spent on other activities, including but not limited to work and/or recreation.

227. The Data Breach has caused Plaintiff DePinto to suffer fear, anxiety, and stress, which has been compounded by Defendant's eighteen-month delay in noticing him of the fact that his Social Security number in conjunction with his date of birth were acquired by criminals as a result of the Data Breach.

228. Plaintiff DePinto anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. In addition, Plaintiff DePinto will continue to be at present and continued increased risk of identity theft and fraud for years to come.

229. Plaintiff DePinto has a continuing interest in ensuring that his Private Information, which upon information and belief, remains in Defendant's possession, is protected and safeguarded from future breaches.

Plaintiff Debbie Bobbitt's Experience

230. Plaintiff Debbie Bobbitt provided her Private Information to Defendant as a condition of receiving healthcare services from Defendant which was then entered into Defendant's computer system and maintained by Defendant.

231. Plaintiff Debbie Bobbitt reasonably understood and expected that Defendant would safeguard her Private Information and timely and adequately notify her in the event of a data breach. Plaintiff Debbie Bobbitt would not have allowed Defendant, or anyone in Defendant's position, to maintain her Private Information if she believed that Defendant would fail to implement reasonable and industry standard practices to safeguard that information from unauthorized access.

232. Plaintiff Debbie Bobbitt received a Notice letter dated June 6, 2023 from Defendant informing her that his Private Information had been compromised in the Data Breach. The Notice letter stated that Plaintiff Debbie Bobbitt's date of birth, device description, medical history, account number, address, dates of service, and name was accessed in the Data Breach.

233. Recognizing the present, immediate, and substantially increased risk of harm Plaintiff Debbie Bobbitt faces, Defendant offered her a twelve-month subscription to a credit monitoring service. The Notice letter Plaintiff Debbie Bobbitt received also cautioned her to "remain vigilant by reviewing account statements and monitoring your credit report for unauthorized activity, especially activity that may indicate fraud and identity theft."

234. Plaintiff Debbie Bobbitt greatly values her privacy and Private Information and

takes reasonable steps to maintain the confidentiality of her Private Information. Plaintiff Debbie Bobbitt is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

235. Plaintiff Debbie Bobbitt stores any and all documents containing Private Information in a secure location and destroys any documents she receives in the mail that contain any Private Information or that may contain any information that could otherwise be used to compromise her identity and credit card accounts. Moreover, she diligently chooses unique usernames and passwords for her various online accounts.

236. To Plaintiff Debbie Bobbitt's knowledge, her PII has not been compromised in a prior data breach.

237. As a result of the Data Breach, Plaintiff Debbie Bobbitt has spent approximately 5-10 hours on necessary mitigation efforts in response to the Data Breach. This is valuable time that Plaintiff spent at Defendant's direction and that she otherwise would have spent on other activities, including but not limited to work and/or recreation.

238. As a consequence of and following the Data Breach, Plaintiff Debbie Bobbitt has experienced an increase in spam phone calls, letters, text messages, and emails.

239. The Data Breach has caused Plaintiff Debbie Bobbitt to suffer fear, anxiety, and stress, which has been compounded by Defendant's eighteen-month delay in noticing her of the fact that her Social Security number in conjunction with her date of birth was acquired by criminals as a result of the Data Breach.

240. Plaintiff Debbie Bobbitt anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. In addition, Plaintiff Debbie Bobbitt will continue to be at present and continued increased risk of identity

theft and fraud for years to come.

241. Plaintiff Debbie Bobbitt has a continuing interest in ensuring that her Private Information, which upon information and belief, remains in Defendant's possession, is protected and safeguarded from future breaches.

Plaintiff Dottie Nikolich's Experience

242. Plaintiff Nikolich provided her Private Information to Defendant as a condition of receiving healthcare services from Defendant which was then entered into Defendant's computer system and maintained by Defendant.

243. Plaintiff Nikolich reasonably understood and expected that Defendant would safeguard her Private Information and timely and adequately notify her in the event of a data breach. Plaintiff Nikolich would not have allowed Defendant, or anyone in Defendant's position, to maintain her Private Information if she believed that Defendant would fail to implement reasonable and industry standard practices to safeguard that information from unauthorized access.

244. Plaintiff Nikolich received a Notice letter dated June 6, 2023, from Defendant informing her that her Private Information had been compromised in the Data Breach. The Notice letter stated that Plaintiff Nikolich's full name, health benefits and enrollment information, and medical history was accessed in the Data Breach.

245. Recognizing the present, immediate, and substantially increased risk of harm Plaintiff Nikolich faces, Defendant offered her a twelve-month subscription to a credit monitoring service. The Notice letter Plaintiff Nikolich received also cautioned her to "remain vigilant by reviewing account statements and monitoring your credit report for unauthorized activity, especially activity that may indicate fraud and identity theft."

246. Plaintiff Nikolich greatly values her privacy and Private Information and takes reasonable steps to maintain the confidentiality of her Private Information. Plaintiff Nikolich is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

247. Plaintiff Nikolich stores any and all documents containing Private Information in a secure location and destroys any documents she receives in the mail that contain any Private Information or that may contain any information that could otherwise be used to compromise her identity and credit card accounts. Moreover, she diligently chooses unique usernames and passwords for her various online accounts.

248. To Plaintiff Nikolich's knowledge, her PII has not been compromised in a prior data breach.

249. As a result of the Data Breach, Plaintiff Nikolich has spent time researching the Data Breach, verifying the legitimacy of the Notice letter, signing up for the credit monitoring service, reviewing her financial accounts, monitoring her credit report, and other necessary mitigation efforts. This is valuable time that Plaintiff spent at Defendant's direction and that she otherwise would have spent on other activities, including but not limited to work and/or recreation.

250. As a consequence of and following the Data Breach, Plaintiff Nikolich received a letter from the IRS notifying her that an unauthorized third party filed tax returns with her personal information. To protect her social security number and the integrity of her tax returns, Plaintiff Nikolich is now required to input a specific PIN number to confirm her identity.

251. The Data Breach has caused Plaintiff Nikolich to suffer fear, anxiety, and stress, which has been compounded by Defendant's eighteen-month delay in noticing her of the fact that

her sensitive personal information was acquired by criminals as a result of the Data Breach.

252. Plaintiff Nikolich anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. In addition, Plaintiff Nikolich will continue to be at present and continued increased risk of identity theft and fraud for years to come.

253. Plaintiff Nikolich has a continuing interest in ensuring that her Private Information, which upon information and belief, remains in Defendant's possession, is protected and safeguarded from future breaches.

Plaintiff Sabrina Munoz's Experience

254. Plaintiff Munoz provided her Private Information to Defendant as a condition of receiving healthcare services from Defendant which was then entered into Defendant's computer system and maintained by Defendant.

255. Plaintiff Munoz reasonably understood and expected that Defendant would safeguard her Private Information and timely and adequately notify her in the event of a data breach. Plaintiff Munoz would not have allowed Defendant, or anyone in Defendant's position, to maintain her Private Information if she believed that Defendant would fail to implement reasonable and industry standard practices to safeguard that information from unauthorized access.

256. Plaintiff Munoz received a Notice letter dated June 6, 2023, from Defendant informing her that her Private Information had been compromised in the Data Breach. The Notice letter stated that Plaintiff Munoz's full name, address, email address, dates of service, telephone numbers, patient account number, and medical history was accessed in the Data Breach.

257. Recognizing the present, immediate, and substantially increased risk of harm

Plaintiff Munoz faces, Defendant offered her a twelve-month subscription to a credit monitoring service. The Notice letter Plaintiff Munoz received also cautioned her to "remain vigilant by reviewing account statements and monitoring your credit report for unauthorized activity, especially activity that may indicate fraud and identity theft."

258. Plaintiff Munoz greatly values her privacy and Private Information and takes reasonable steps to maintain the confidentiality of her Private Information. Plaintiff Munoz is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

259. Plaintiff Munoz stores any and all documents containing Private Information in a secure location and destroys any documents she receives in the mail that contain any Private Information or that may contain any information that could otherwise be used to compromise her identity and credit card accounts. Moreover, she diligently chooses unique usernames and passwords for her various online accounts.

260. As a result of the Data Breach, Plaintiff Munoz has spent time researching the Data Breach, verifying the legitimacy of the Notice letter, signing up for the credit monitoring service, reviewing her financial accounts, monitoring her credit report, freezing her credit for $13.99 per month with Experian, and other necessary mitigation efforts. She constantly monitors her accounts every day. This is valuable time that Plaintiff spent at Defendant's direction and that she otherwise would have spent on other activities, including but not limited to work and/or recreation.

261. As a consequence of and following the Data Breach, Plaintiff Munoz has received alerts notifying her that her social security number has been compromised and her email address has been found on the dark web. Since the data breach, Plaintiff Munoz has also received

alerts notifying her of fraudulent purchases and transactions being made in her name, including the unauthorized purchase of a car using her personal information.

262. The Data Breach has caused Plaintiff Munoz to suffer fear, anxiety, and stress, which has been compounded by Defendant's eighteen-month delay in noticing her of the fact that her sensitive personal information was acquired by criminals as a result of the Data Breach.

263. Plaintiff Munoz anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. In addition, Plaintiff Munoz will continue to be at present and continued increased risk of identity theft and fraud for years to come.

264. Plaintiff Munoz has a continuing interest in ensuring that her Private Information, which upon information and belief, remains in Defendant's possession, is protected and safeguarded from future breaches.

Plaintiff Hilary French's Experience

265. Plaintiff French provided her Private Information to Defendant as a condition of receiving healthcare services from Defendant which was then entered into Defendant's computer system and maintained by Defendant.

266. Plaintiff French reasonably understood and expected that Defendant would safeguard her Private Information and timely and adequately notify her in the event of a data breach. Plaintiff French would not have allowed Defendant, or anyone in Defendant's position, to maintain her Private Information if she believed that Defendant would fail to implement reasonable and industry standard practices to safeguard that information from unauthorized access.

267. Plaintiff French received a Notice letter dated June 6, 2023, from Defendant

informing her that her Private Information had been compromised in the Data Breach. The Notice letter stated that Plaintiff French's social security number, medical records, address, prescriptions, and other sensitive personal information was accessed in the Data Breach.

268. Recognizing the present, immediate, and substantially increased risk of harm Plaintiff French faces, Defendant offered her a twelve-month subscription to a credit monitoring service. The Notice letter Plaintiff French received also cautioned her to "remain vigilant by reviewing account statements and monitoring your credit report for unauthorized activity, especially activity that may indicate fraud and identity theft."

269. Plaintiff French greatly values her privacy and Private Information and takes reasonable steps to maintain the confidentiality of her Private Information. Plaintiff French is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

270. Plaintiff French stores any and all documents containing Private Information in a secure location and destroys any documents she receives in the mail that contain any Private Information or that may contain any information that could otherwise be used to compromise her identity and credit card accounts. Moreover, she diligently chooses unique usernames and passwords for her various online accounts.

271. As a result of the Data Breach, Plaintiff French has spent 1-2 hours per week on mitigation activities in response to the Data Breach including but not limited to: researching the Data Breach, signing up for the credit monitoring service, reviewing her financial accounts, monitoring her credit report, and other necessary mitigation efforts. This is valuable time that Plaintiff spent at Defendant's direction and that she otherwise would have spent on other activities, including but not limited to work and/or recreation.

272. As a consequence of and following the Data Breach, Plaintiff French has experienced a severe increase in suspicious calls, emails, and text messages that resulted in her having to get a new phone number and email address due to the high volume of spam calls and suspicious messages.

273. The Data Breach has caused Plaintiff French to suffer fear, anxiety, and stress, which has been compounded by Defendant's eighteen-month delay in noticing her of the fact that her social security number and sensitive personal information was acquired by criminals as a result of the Data Breach.

274. Plaintiff French anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. In addition, Plaintiff French will continue to be at present and continued increased risk of identity theft and fraud for years to come.

275. Plaintiff French has a continuing interest in ensuring that her Private Information, which upon information and belief, remains in Defendant's possession, is protected and safeguarded from future breaches.

Plaintiff Elisa Stroffolino's Experience

276. Plaintiff Stroffolino provided her Private Information to Defendant as a condition of receiving healthcare services from Defendant which was then entered into Defendant's computer system and maintained by Defendant.

277. Plaintiff Stroffolino reasonably understood and expected that Defendant would safeguard her Private Information and timely and adequately notify her in the event of a data breach. Plaintiff Stroffolino would not have allowed Defendant, or anyone in Defendant's position, to maintain her Private Information if she believed that Defendant would fail to

implement reasonable and industry standard practices to safeguard that information from unauthorized access.

278. Plaintiff Stroffolino received a Notice letter dated June 6, 2023, from Defendant informing her that her Private Information had been compromised in the Data Breach. The Notice letter stated that Plaintiff Stroffolino's patient account number, patient email address, and patient name were accessed in the Data Breach.

279. Recognizing the present, immediate, and substantially increased risk of harm Plaintiff Stroffolino faces, Defendant offered her a twelve-month subscription to a credit monitoring service. The Notice letter Plaintiff Stroffolino received also cautioned her to "remain vigilant by reviewing account statements and monitoring your credit report for unauthorized activity, especially activity that may indicate fraud and identity theft."

280. Plaintiff Stroffolino greatly values her privacy and Private Information and takes reasonable steps to maintain the confidentiality of her Private Information. Plaintiff Stroffolino is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

281. Plaintiff Stroffolino stores any and all documents containing Private Information in a secure location and destroys any documents she receives in the mail that contain any Private Information or that may contain any information that could otherwise be used to compromise her identity and credit card accounts. Moreover, she diligently chooses unique usernames and passwords for her various online accounts.

282. As a result of the Data Breach, Plaintiff Stroffolino has spent significant time on activities in response to the Data Breach, including but not limited to: researching the Data Breach, verifying the legitimacy of the Notice letter, signing up for the credit monitoring service,

reviewing her financial accounts, monitoring her credit report, and other necessary mitigation efforts. This is valuable time that Plaintiff spent at Defendant's direction and that she otherwise would have spent on other activities, including but not limited to work and/or recreation.

283. The Data Breach has caused Plaintiff Stroffolino to suffer fear, anxiety, and stress, which has been compounded by Defendant's eighteen-month delay in noticing her of the fact that her sensitive personal information was acquired by criminals as a result of the Data Breach.

284. Plaintiff Stroffolino anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. In addition, Plaintiff Stroffolino will continue to be at present and continued increased risk of identity theft and fraud for years to come.

285. Plaintiff Stroffolino has a continuing interest in ensuring that her Private Information, which upon information and belief, remains in Defendant's possession, is protected and safeguarded from future breaches.

Plaintiff Amy Clark's Experience

286. Plaintiff Clark provided her Private Information to Defendant as a condition of receiving healthcare services from Defendant which was then entered into Defendant's computer system and maintained by Defendant.

287. Plaintiff Clark reasonably understood and expected that Defendant would safeguard her Private Information and timely and adequately notify her in the event of a data breach. Plaintiff Clark would not have allowed Defendant, or anyone in Defendant's position, to maintain her Private Information if she believed that Defendant would fail to implement reasonable and industry standard practices to safeguard that information from unauthorized

access.

288. Plaintiff Clark received a Notice letter dated June 6, 2023, from Defendant informing her that her Private Information had been compromised in the Data Breach. The Notice letter stated that Plaintiff Clark's full name, date of birth, medical history, patient account number, and dates of service were accessed in the Data Breach.

289. Recognizing the present, immediate, and substantially increased risk of harm Plaintiff Clark faces, Defendant offered her a twelve-month subscription to a credit monitoring service. The Notice letter Plaintiff Clark received also cautioned her to "remain vigilant by reviewing account statements and monitoring your credit report for unauthorized activity, especially activity that may indicate fraud and identity theft."

290. Plaintiff Clark greatly values her privacy and Private Information and takes reasonable steps to maintain the confidentiality of her Private Information. Plaintiff Clark is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

291. Plaintiff Clark stores any and all documents containing Private Information in a secure location and destroys any documents she receives in the mail that contain any Private Information or that may contain any information that could otherwise be used to compromise her identity and credit card accounts. Moreover, she diligently chooses unique usernames and passwords for her various online accounts.

292. As a result of the Data Breach, Plaintiff Clark has spent approximately 20 hours on activities in response to the Data Breach, including but not limited to: researching the Data Breach, verifying the legitimacy of the Notice letter, reviewing her financial accounts, monitoring her credit report, contacting the IRS, and other necessary mitigation efforts. This is valuable time

that Plaintiff spent at Defendant's direction and that she otherwise would have spent on other activities, including but not limited to work and/or recreation.

293. As a consequence of and following the Data Breach, Plaintiff Clark has experienced actual identity theft confirmed by a notification she recently received from the IRS notifying her that an unauthorized third party filed a tax return in her name.

294. The Data Breach has caused Plaintiff Clark to suffer fear, anxiety, and stress, which has been compounded by Defendant's eighteen-month delay in noticing her of the fact that her sensitive personal information was acquired by criminals as a result of the Data Breach.

295. Plaintiff Clark anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. In addition, Plaintiff Clark will continue to be at present and continued increased risk of identity theft and fraud for years to come.

296. Plaintiff Clark has a continuing interest in ensuring that her Private Information, which upon information and belief, remains in Defendant's possession, is protected and safeguarded from future breaches.

Plaintiff Reginald Reese's Experience

297. Plaintiff Reese provided his Private Information to Defendant as a condition of receiving healthcare services from Defendant which was then entered into Defendant's computer system and maintained by Defendant.

298. Plaintiff Reese reasonably understood and expected that Defendant would safeguard his Private Information and timely and adequately notify him in the event of a data breach. Plaintiff Reese would not have allowed Defendant, or anyone in Defendant's position, to maintain his Private Information if he believed that Defendant would fail to implement reasonable

and industry standard practices to safeguard that information from unauthorized access.

299. Plaintiff Reese received a Notice letter dated June 6, 2023, from Defendant informing him that his Private Information had been compromised in the Data Breach. The Notice letter stated that Plaintiff Reese's patient account number and other sensitive medical information was accessed in the Data Breach.

300. Recognizing the present, immediate, and substantially increased risk of harm Plaintiff Reese faces, Defendant offered him a twelve-month subscription to a credit monitoring service. The Notice letter Plaintiff Reese received also cautioned him to "remain vigilant by reviewing account statements and monitoring your credit report for unauthorized activity, especially activity that may indicate fraud and identity theft."

301. Plaintiff Reese greatly values his privacy and Private Information and takes reasonable steps to maintain the confidentiality of his Private Information. Plaintiff Reese is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

302. Plaintiff Reese stores any and all documents containing Private Information in a secure location and destroys any documents he receives in the mail that contain any Private Information or that may contain any information that could otherwise be used to compromise his identity and credit card accounts. Moreover, he diligently chooses unique usernames and passwords for his various online accounts.

303. As a result of the Data Breach, Plaintiff Reese has spent significant time on activities in response to the Data Breach, including but not limited to: constantly monitoring his financial accounts and reviewing his credit report multiple times a day, along with implementing other necessary mitigation efforts. This is valuable time that Plaintiff Reese spent at Defendant's

direction and that he otherwise would have spent on other activities, including but not limited to work and/or recreation.

304. As a consequence of and following the Data Breach, Plaintiff Reese has experienced identity theft, including an attempt by an unauthorized third-party to open a credit card and apply for a car loan in his name. He also noticed suspicious charges for laptops on his financial accounts and strange mailing addresses listed on his credit report for places that he has never lived or visited.

305. After the Data Breach, Plaintiff Reese also began receiving phishing calls and emails from scammers in foreign countries posing as officials to solicit money from him.

306. The Data Breach has caused Plaintiff Reese to suffer fear, anxiety, and stress, which has been compounded by Defendant's eighteen-month delay in notifying him of the fact that his sensitive personal information was acquired by criminals as a result of the Data Breach.

307. Plaintiff Reese anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. In addition, Plaintiff Reese will continue to be at present and continued increased risk of identity theft and fraud for years to come.

308. Plaintiff Reese has a continuing interest in ensuring that his Private Information, which upon information and belief, remains in Defendant's possession, is protected and safeguarded from future breaches.

Plaintiff Rita May's Experience

309. Plaintiff May provided her Private Information to Defendant as a condition of receiving healthcare services from Defendant which was then entered into Defendant's computer system and maintained by Defendant.

310. Plaintiff May reasonably understood and expected that Defendant would safeguard her Private Information and timely and adequately notify her in the event of a data breach. Plaintiff May would not have allowed Defendant, or anyone in Defendant's position, to maintain her Private Information if she believed that Defendant would fail to implement reasonable and industry standard practices to safeguard that information from unauthorized access.

311. Plaintiff May received a Notice letter dated June 6, 2023 from Defendant informing her that her Private Information had been compromised in the Data Breach. The Notice letter stated that Plaintiff May's full name, address, patient account number, dates of service, email address, and telephone number was accessed in the Data Breach.

312. Recognizing the present, immediate, and substantially increased risk of harm Plaintiff May faces, Defendant offered her a twelve-month subscription to a credit monitoring service. The Notice letter Plaintiff May received also cautioned her to "remain vigilant by reviewing account statements and monitoring your credit report for unauthorized activity, especially activity that may indicate fraud and identity theft."

313. Plaintiff May greatly values her privacy and Private Information and takes reasonable steps to maintain the confidentiality of her Private Information. Plaintiff May is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

314. Plaintiff May stores any and all documents containing Private Information in a secure location and destroys any documents she receives in the mail that contain any Private Information or that may contain any information that could otherwise be used to compromise her identity and credit card accounts. Moreover, she diligently chooses unique usernames and

passwords for her various online accounts.

315. As a result of the Data Breach, Plaintiff May has spent approximately 1 hour on activities in response to the Data Breach, including but not limited to: verifying the legitimacy of the Notice letter, signing up for the credit monitoring service, and other necessary mitigation efforts. This is valuable time that Plaintiff spent at Defendant's direction and that she otherwise would have spent on other activities, including but not limited to work and/or recreation.

316. As a consequence of and following the Data Breach, Plaintiff May has experienced a substantial increase in the number of spam calls and emails she receives.

317. The Data Breach has caused Plaintiff May to suffer fear, anxiety, and stress, which has been compounded by Defendant's eighteen-month delay in noticing her of the fact that her Private Information was acquired by criminals as a result of the Data Breach.

318. Plaintiff May anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. In addition, Plaintiff May will continue to be at present and continued increased risk of identity theft and fraud for years to come.

319. Plaintiff May has a continuing interest in ensuring that her Private Information, which upon information and belief, remains in Defendant's possession, is protected and safeguarded from future breaches.

Plaintiff Bonnie Bennett's Experience

320. Plaintiff Bonnie Bennett provided her Private Information to Defendant as a condition of receiving healthcare services from Defendant which was then entered into Defendant's computer system and maintained by Defendant.

321. Plaintiff Bonnie Bennett reasonably understood and expected that Defendant

would safeguard her Private Information and timely and adequately notify her in the event of a data breach. Plaintiff Bonnie Bennett would not have allowed Defendant, or anyone in Defendant's position, to maintain her Private Information if she believed that Defendant would fail to implement reasonable and industry standard practices to safeguard that information from unauthorized access.

322. Plaintiff Bonnie Bennett received a Notice letter dated May 22, 2023 from Defendant informing her that her Private Information had been compromised in the Data Breach. The Notice letter stated that Plaintiff Bonnie Bennett's full name, address, financial account information, contact information, and medical information and treatment information was accessed in the Data Breach.

323. Recognizing the present, immediate, and substantially increased risk of harm Plaintiff Bonnie Bennettt faces, Defendant offered her a twelve-month subscription to a credit monitoring service. The Notice letter Plaintiff Bonnie Bennett received also cautioned her to "remain vigilant by reviewing account statements and monitoring your credit report for unauthorized activity, especially activity that may indicate fraud and identity theft."

324. Plaintiff Bonnie Bennett greatly values her privacy and Private Information and takes reasonable steps to maintain the confidentiality of her Private Information. Plaintiff Bonnie Bennett is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

325. Plaintiff Bonnie Bennett stores any and all documents containing Private Information in a secure location and destroys any documents she receives in the mail that contain any Private Information or that may contain any information that could otherwise be used to compromise her identity and credit card accounts. Moreover, she diligently chooses unique

usernames and passwords for her various online accounts.

326. As a result of the Data Breach, Plaintiff Bonnie Bennett has spent approximately 20 hours on activities in response to the Data Breach, including but not limited to: researching the Data Breach, verifying the legitimacy of the Notice letter, reaching out to attorneys, and other necessary mitigation efforts. This is valuable time that Plaintiff spent at Defendant's direction and that she otherwise would have spent on other activities, including but not limited to work and/or recreation.

327. As a consequence of and following the Data Breach, Plaintiff Bonnie Bennett has experienced fraud to her email account as well as her bank account resulting in both accounts becoming locked, increase spam calls and text messages as well.

328. The Data Breach has caused Plaintiff Bonnie Bennett to suffer fear, anxiety, and stress, which has been compounded by Defendant's eighteen-month delay in noticing her of the fact that her Social Security number in conjunction with her date of birth was acquired by criminals as a result of the Data Breach.

329. Plaintiff Bonnie Bennett anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. In addition, Plaintiff Bonnie Bennett will continue to be at present and continued increased risk of identity theft and fraud for years to come.

330. Plaintiff Bonnie Bennett has a continuing interest in ensuring that her Private Information, which upon information and belief, remains in Defendant's possession, is protected and safeguarded from future breaches.

Plaintiff Tammie Creek's Experience

331. Plaintiff Creek provided her Private Information to Defendant as a condition of

receiving healthcare services from Defendant which was then entered into Defendant's computer system and maintained by Defendant.

332. Plaintiff Creek reasonably understood and expected that Defendant would safeguard her Private Information and timely and adequately notify her in the event of a data breach. Plaintiff Creek would not have allowed Defendant, or anyone in Defendant's position, to maintain her Private Information if she believed that Defendant would fail to implement reasonable and industry standard practices to safeguard that information from unauthorized access.

333. Plaintiff Creek received a Notice letter dated June 6, 2023 from Defendant informing her that her Private Information had been compromised in the Data Breach. The Notice letter stated that Plaintiff Creek full name, date of birth, device descriptions, health insurance policy number or subscriber number, medical history, patient account number, telephone number, and Social Security number was accessed in the Data Breach.

334. Recognizing the present, immediate, and substantially increased risk of harm Plaintiff Creek faces, Defendant offered her a twelve-month subscription to a credit monitoring service. The Notice letter Plaintiff Creek received also cautioned her to "remain vigilant by reviewing account statements and monitoring your credit report for unauthorized activity, especially activity that may indicate fraud and identity theft."

335. Plaintiff Creek greatly values her privacy and Private Information and takes reasonable steps to maintain the confidentiality of her Private Information. Plaintiff Creek is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

336. Plaintiff Creek stores any and all documents containing Private Information in a

secure location and destroys any documents she receives in the mail that contain any Private Information or that may contain any information that could otherwise be used to compromise her identity and credit card accounts. Moreover, she diligently chooses unique usernames and passwords for her various online accounts.

337. As a result of the Data Breach, Plaintiff Creek has spent approximately 2 hours on activities in response to the Data Breach, including but not limited to: verifying the legitimacy of the Notice letter, reviewing her bank accounts, replacing her Discover credit card, and other necessary mitigation efforts. This is valuable time that Plaintiff spent at Defendant's direction and that she otherwise would have spent on other activities, including but not limited to work and/or recreation.

338. As a consequence of and following the Data Breach, Plaintiff Creek has experienced fraudulent charges on her Discover card which required her to replace her Discover card. Plaintiff Creek additionally has experienced a substantial increase in the number of spam calls and emails she receives.

339. The Data Breach has caused Plaintiff Creek to suffer fear, anxiety, and stress, which has been compounded by Defendant's eighteen-month delay in noticing her of the fact that her Social Security number in conjunction with her date of birth was acquired by criminals as a result of the Data Breach.

340. Plaintiff Creek anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. In addition, Plaintiff Creek will continue to be at present and continued increased risk of identity theft and fraud for years to come.

341. Plaintiff Creek has a continuing interest in ensuring that her Private Information,

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

Plaintiff Sonya Albert's Experience

342. Plaintiff Albert provided her Private Information to Defendant as a condition of receiving healthcare services from Defendant which was then entered into Defendant's computer system and maintained by Defendant.

343. Plaintiff Albert reasonably understood and expected that Defendant would safeguard her Private Information and timely and adequately notify her in the event of a data breach. Plaintiff Albert would not have allowed Defendant, or anyone in Defendant's position, to maintain her Private Information if she believed that Defendant would fail to implement reasonable and industry standard practices to safeguard that information from unauthorized access.

344. Plaintiff Albert received a Notice letter dated June 6, 2023 from Defendant informing her that her Private Information had been compromised in the Data Breach. The Notice letter stated that Plaintiff Albert's full name, address, date of birth, device descriptions, patient account number, dates of service, email address, and telephone number was accessed in the Data Breach.

345. Recognizing the present, immediate, and substantially increased risk of harm Plaintiff Albert faces, Defendant offered her a twelve-month subscription to a credit monitoring service. The Notice letter Plaintiff Albert received also cautioned her to "remain vigilant by reviewing account statements and monitoring your credit report for unauthorized activity, especially activity that may indicate fraud and identity theft."

346. Plaintiff Albert greatly values her privacy and Private Information and takes

reasonable steps to maintain the confidentiality of her Private Information. Plaintiff Albert is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

347. Plaintiff Albert stores any and all documents containing Private Information in a secure location and destroys any documents she receives in the mail that contain any Private Information or that may contain any information that could otherwise be used to compromise her identity and credit card accounts. Moreover, she diligently chooses unique usernames and passwords for her various online accounts.

348. As a result of the Data Breach, Plaintiff Albert has spent approximately 24 hours on activities in response to the Data Breach, including but not limited to: researching the Data Breach, verifying the legitimacy of the Notice letter, reviewing her bank accounts, monitoring her credit report, changing her passwords, replacing her debit cards, and other necessary mitigation efforts. This is valuable time that Plaintiff spent at Defendant's direction and that she otherwise would have spent on other activities, including but not limited to work and/or recreation.

349. As a consequence of and following the Data Breach, Plaintiff Albert has experienced fraudulent charges to her debit cards in late-2021, requiring Plaintiff to replace her debit cards. Plaintiff has also experienced a substantial increase in the number of spam calls, emails, and text messages she receives.

350. The Data Breach has caused Plaintiff Albert to suffer fear, anxiety, and stress, which has been compounded by Defendant's eighteen-month delay in noticing her of the fact that her Private Information was acquired by criminals as a result of the Data Breach.

351. Plaintiff Albert anticipates spending considerable time and money on an ongoing

basis to try to mitigate and address harms caused by the Data Breach. In addition, Plaintiff Albert will continue to be at present and continued increased risk of identity theft and fraud for years to come.

352. Plaintiff Albert has a continuing interest in ensuring that her Private Information, which upon information and belief, remains in Defendant's possession, is protected and safeguarded from future breaches.

Plaintiff Chad Hohenbery's Experience

353. Plaintiff Chad Hohenbery provided his Private Information to Defendant as a condition of his employment with Defendant which was then entered into Defendant's computer system and maintained by Defendant.

354. Plaintiff Hohenbery reasonably understood and expected that Defendant would safeguard his Private Information and timely and adequately notify him in the event of a data breach. Plaintiff Hohenbery would not have allowed Defendant, or anyone in Defendant's position, to maintain his Private Information if he believed that Defendant would fail to implement reasonable and industry standard practices to safeguard that information from unauthorized access.

355. Plaintiff Hohenbery received a Notice letter, dated June 6, 2023, from Defendant, informing him that his Private Information had been compromised in the Data Breach. The Notice letter stated that Plaintiff Hohenbery's name, date of birth, address, dates of service, email, and telephone number were accessed in the Data Breach.

356. Recognizing the present, immediate, and substantially increased risk of harm Plaintiff Hohenbery faces, Defendant offered him a twelve-month subscription to a credit monitoring service. The Notice letter Plaintiff Hohenbery received also cautioned his to "remain

vigilant by reviewing account statements and monitoring your credit report for unauthorized activity, especially activity that may indicate fraud and identity theft."

357. Plaintiff Hohenbery greatly values his privacy and Private Information and takes reasonable steps to maintain the confidentiality of his Private Information. Plaintiff Hohenbery is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

358. Plaintiff Hohenbery stores any and all documents containing Private Information in a secure location and destroys any documents he receives in the mail that contain any Private Information or that may contain any information that could otherwise be used to compromise his identity and credit card accounts. Moreover, he diligently chooses unique usernames and passwords for his various online accounts.

359. To Plaintiff Hohenbery's knowledge, his PII has not been compromised in a prior data breach.

360. As a result of the Data Breach, Plaintiff Hohenbery has spent between 8-12 hours in an attempt to mitigate his damages so far. This time has been spent researching the Data Breach, verifying the legitimacy of the Notice letter, reviewing his bank accounts, monitoring his credit report, and other necessary efforts. This is valuable time that Plaintiff spent at Defendant's direction and that he otherwise would have spent on other activities, including but not limited to work and/or recreation.

361. In addition to time, Plaintiff has experienced actual fraud resulting from the Data Breach when on four separate occasions recently he has noticed suspicious transactions on the bank account linked to his Cash App account. These charges, totaling roughly $200, were never reimbursed. Further, an unidentified person filed for unemployment benefits using Plaintiff

Hohenbery's information in January of 2023. Plaintiff Hohenbery had to spend significant time working with the office of unemployment benefits in order to remedy the fraud.

362. The Data Breach has caused Plaintiff Hohenbery to suffer fear, anxiety, and stress, which has been compounded by Defendant's eighteen-month delay in noticing his of the fact that his medical information in conjunction with his date of birth was acquired by criminals as a result of the Data Breach.

363. Plaintiff Hohenbery anticipates spending even further considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. In addition, Plaintiff Hohenbery will continue to be at present and continued increased risk of identity theft and fraud for years to come.

364. Plaintiff Hohenbery has a continuing interest in ensuring that his Private Information, which upon information and belief, remains in Defendant's possession, is protected and safeguarded from future breaches.

Plaintiff Colleen Rickard's Experience

365. Plaintiff Colleen Rickard provided her Private Information to Defendant as a condition of receiving healthcare services from Defendant which was then entered into Defendant's computer system and maintained by Defendant.

366. Plaintiff Rickard reasonably understood and expected that Defendant would safeguard her Private Information and timely and adequately notify her in the event of a data breach. Plaintiff Rickard would not have allowed Defendant, or anyone in Defendant's position, to maintain her Private Information if she believed that Defendant would fail to implement reasonable and industry standard practices to safeguard that information from unauthorized access.

367. Plaintiff Rickard received a Notice letter, dated June 6, 2023, from Defendant, informing her that her Private Information had been compromised in the Data Breach. The Notice letter stated that Plaintiff Rickard's name, date of birth, medical device descriptions, patient account number, address, dates of service, email, and telephone number were accessed in the Data Breach.

368. Recognizing the present, immediate, and substantially increased risk of harm Plaintiff Rickard faces, Defendant offered her a twelve-month subscription to a credit monitoring service. The Notice letter Plaintiff Rickard received also cautioned her to "remain vigilant by reviewing account statements and monitoring your credit report for unauthorized activity, especially activity that may indicate fraud and identity theft."

369. Plaintiff Rickard greatly values her privacy and Private Information and takes reasonable steps to maintain the confidentiality of her Private Information. Plaintiff Rickard is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

370. Plaintiff Rickard stores any and all documents containing Private Information in a secure location and destroys any documents she receives in the mail that contain any Private Information or that may contain any information that could otherwise be used to compromise her identity and credit card accounts. Moreover, she diligently chooses unique usernames and passwords for her various online accounts.

371. To Plaintiff Rickard's knowledge, her PII has not been compromised in a prior data breach.

372. As a result of the Data Breach, Plaintiff Rickard has spent more than 10 hours in an attempt to mitigate her damages so far. This time has been spent researching the Data Breach,

verifying the legitimacy of the Notice letter, signing up for credit monitoring and identity theft protection services like LifeLock, reviewing her bank accounts, monitoring her credit report, implementing credit freezes, driving to and from her bank when required to attend meeting in person to correct her accounts and information, and other necessary efforts. This is valuable time that Plaintiff spent at Defendant's direction and that she otherwise would have spent on other activities, including but not limited to work and/or recreation.

373. In addition to time, Plaintiff has spent money as a direct result of the Data Breach in the form of her paid subscription to LifeLock for identity theft protection and credit monitoring services, as well as money spent on gasoline to travel to and from the bank at least 3 times to correct information and statements compromised as a result of the Data Breach.

374. The Data Breach has caused Plaintiff Rickard to suffer fear, anxiety, and stress, which has been compounded by Defendant's eighteen-month delay in noticing her of the fact that her medical information in conjunction with her date of birth was acquired by criminals as a result of the Data Breach.

375. Plaintiff Rickard anticipates spending even further considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. In addition, Plaintiff Rickard will continue to be at present and continued increased risk of identity theft and fraud for years to come.

376. Plaintiff Rickard has a continuing interest in ensuring that her Private Information, which upon information and belief, remains in Defendant's possession, is protected and safeguarded from future breaches.

Plaintiff Kristina Accardo's Experience

377. Plaintiff Accardo provided her Private Information to Defendant as a condition

of receiving services from Defendant which was then entered into Defendant's computer system and maintained by Defendant.

378. Plaintiff Accardo reasonably understood and expected that Defendant would safeguard her Private Information and timely and adequately notify her in the event of a data breach. Plaintiff Accardo would not have allowed Defendant, or anyone in Defendant's position, to maintain her Private Information if she believed that Defendant would fail to implement reasonable and industry standard practices to safeguard that information from unauthorized access.

379. Plaintiff Accardo received a Notice letter dated June 6, 2023, from Defendant informing her that his Private Information had been compromised in the Data Breach. The Notice letter stated that Plaintiff Accardo's full name, address, email address, phone numbers, and device description was accessed in the Data Breach.

380. Recognizing the present, immediate, and substantially increased risk of harm Plaintiff Accardo faces, Defendant offered her a twelve-month subscription to a credit monitoring service. The Notice letter Plaintiff Accardo received also cautioned her to "remain vigilant by reviewing account statements and monitoring your credit report for unauthorized activity, especially activity that may indicate fraud and identity theft."

381. Plaintiff Accardo greatly values her privacy and Private Information and takes reasonable steps to maintain the confidentiality of her Private Information. Plaintiff Accardo is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

382. Plaintiff Accardo stores any and all documents containing Private Information in a secure location and destroys any documents she receives in the mail that contain any Private

Information or that may contain any information that could otherwise be used to compromise her identity and credit card accounts. Moreover, she diligently chooses unique usernames and passwords for her various online accounts.

383. As a result of the Data Breach, Plaintiff Accardo has spent approximately [X] hours researching the Data Breach, signing up, and paying, for credit monitoring services through LifeLock, monitoring her credit report, freezing her credit with all three credit bureaus, and dealing with a substantial increase in spam phone calls and emails following the data breach, and other necessary mitigation efforts. This is valuable time that Plaintiff spent at Defendant's direction and that she otherwise would have spent on other activities, including but not limited to work and/or recreation.

384. As a consequence of and following the Data Breach, Plaintiff Accardo has experienced a substantial increase in the amount of spam calls received on her home phone, the phone number she provided to Apria. Ultimately, as a result of the increased spam calls, Plaintiff Accardo cancelled her home phone line. In addition, Plaintiff Accardo experienced a substantial increase in spam emails to her work email address, which she had provided to Apria, following the data breach.

385. The Data Breach has caused Plaintiff Accardo to suffer fear, anxiety, and stress, which has been compounded by Defendant's eighteen-month delay in noticing her of the fact that her Private Information was acquired by criminals as a result of the Data Breach.

386. Plaintiff Accardo anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. In addition, Plaintiff Accardo will continue to be at present and continued increased risk of identity theft and fraud for years to come.

387. Plaintiff Accardo has a continuing interest in ensuring that her Private Information, which upon information and belief, remains in Defendant's possession, is protected and safeguarded from future breaches.

Plaintiff Roger Winstanley's Experience

388. Plaintiff Winstanley provided his Private Information to Defendant as a condition of receiving healthcare services from Defendant which was then entered into Defendant's computer system and maintained by Defendant.

389. Plaintiff Winstanley reasonably understood and expected that Defendant would safeguard his Private Information and timely and adequately notify him in the event of a data breach. Plaintiff Winstanley would not have allowed Defendant, or anyone in Defendant's position, to maintain his Private Information if he believed that Defendant would fail to implement reasonable and industry standard practices to safeguard that information from unauthorized access.

390. Plaintiff Winstanley received a Notice letter dated June 6, 2023 from Defendant informing him/her that his Private Information had been compromised in the Data Breach. The Notice letter stated that Plaintiff Winstanley's device descriptions, account number, and full name were accessed in the Data Breach.

391. Recognizing the present, immediate, and substantially increased risk of harm Plaintiff Winstanley faces, Defendant offered him/her a twelve-month subscription to a credit monitoring service. The Notice letter Plaintiff Winstanley received also cautioned him/her to "remain vigilant by reviewing account statements and monitoring your credit report for unauthorized activity, especially activity that may indicate fraud and identity theft."

392. Plaintiff Winstanley greatly values his privacy and Private Information and takes

reasonable steps to maintain the confidentiality of his Private Information. Plaintiff Winstanley is very concerned about the privacy of his health information, identity theft and fraud, and the consequences of such identity theft and fraud resulting from the Data Breach.

393. Plaintiff Winstanley stores any and all documents containing Private Information in a secure location and destroys any documents he receives in the mail that contain any Private Information or that may contain any information that could otherwise be used to compromise his identity and credit card accounts. Moreover, he diligently chooses unique user names and passwords for his various online accounts.

394. As a result of the Data Breach, Plaintiff Winstanley has spent at least two hours to date researching the Data Breach, verifying the legitimacy of the Notice letter, reviewing his bank accounts, and monitoring his credit report, changing his passwords and payment account numbers], and other necessary mitigation efforts. This is valuable time that Plaintiff spent at Defendant's direction and that he otherwise would have spent on other activities, including but not limited to work and/or recreation.

395. The Data Breach has caused Plaintiff Winstanley to suffer fear, anxiety, and stress, which has been compounded by Defendant's eighteen-month delay in noticing him of the fact that his Social Security number in conjunction with his date of birth was acquired by criminals as a result of the Data Breach.

396. Plaintiff Winstanley anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. In addition, Plaintiff Winstanley will continue to be at present and continued increased risk of identity theft and fraud for years to come.

397. Plaintiff Winstanley has a continuing interest in ensuring that his Private

Information, which upon information and belief, remains in Defendant's possession, is protected and safeguarded from future breaches.

Plaintiff Paul Kramer's Experience

398. Plaintiff Kramer provided his Private Information to Defendant as a condition of receiving healthcare services from Defendant which was then entered into Defendant's computer system and maintained by Defendant.

399. Plaintiff Kramer reasonably understood and expected that Defendant would safeguard his Private Information and timely and adequately notify him in the event of a data breach. Plaintiff Kramer would not have allowed Defendant, or anyone in Defendant's position, to maintain his Private Information if he believed that Defendant would fail to implement reasonable and industry standard practices to safeguard that information from unauthorized access.

400. Plaintiff Kramer received a Notice letter dated June 6, 2023, from Defendant informing him that his Private Information had been compromised in the Data Breach. The Notice letter stated that Plaintiff Kramer's name, date of birth, device descriptions, patient account number, address, dates of service, email address, and telephone number was accessed in the Data Breach.

401. Recognizing the present, immediate, and substantially increased risk of harm Plaintiff Kramer faces, Defendant offered him a twelve-month subscription to a credit monitoring service. The Notice letter Plaintiff Kramer received also cautioned him to "remain vigilant by reviewing account statements and monitoring your credit report for unauthorized activity, especially activity that may indicate fraud and identity theft."

402. Plaintiff Kramer greatly values his privacy and Private Information and takes

reasonable steps to maintain the confidentiality of his Private Information. Plaintiff Kramer is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

403. Plaintiff Kramer stores any and all documents containing Private Information in a secure location and destroys any documents he receives in the mail that contain any Private Information or that may contain any information that could otherwise be used to compromise his identity and credit card accounts. Moreover, he diligently chooses unique usernames and passwords for his various online accounts.

404. To Plaintiff Kramer's knowledge, his PII has not been compromised in a prior data breach.

405. As a result of the Data Breach, Plaintiff Kramer has spent time on activities in response to the Data Breach, including but not limited to: researching the Data Breach, verifying the legitimacy of the Notice letter, signing up for credit monitoring, reviewing his bank accounts, changing his passwords and payment account numbers, cancelling credit cards, and other necessary mitigation efforts. This is valuable time that Plaintiff spent at Defendant's direction and that he otherwise would have spent on other activities, including but not limited to work and/or recreation.

406. As a consequence of and following the Data Breach, Plaintiff Kramer has experienced fraudulent activity to his accounts and identity theft. Namely, after the Data Breach, Plaintiff experienced fraudulent charges to the credit card he used to pay for Apria supplies. The fraudulent charges were for items such as clothing purchases and medications that Plaintiff did not authorize.

407. The Data Breach has caused Plaintiff Kramer to suffer fear, anxiety, and stress,

which has been compounded by Defendant's eighteen-month delay in noticing him of the fact that his Social Security number in conjunction with his date of birth was acquired by criminals as a result of the Data Breach.

408. Plaintiff Kramer anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. In addition, Plaintiff Kramer will continue to be at present and continued increased risk of identity theft and fraud for years to come.

409. Plaintiff Kramer has a continuing interest in ensuring that his Private Information, which upon information and belief, remains in Defendant's possession, is protected and safeguarded from future breaches.

TOLLING OF THE STATUTE OF LIMITATIONS

410. Any applicable statute of limitations has been tolled by the "delayed discovery" rule, Defendant's knowing and active concealment of the Data Breach, and the misrepresentations and omissions alleged herein. Plaintiffs did not know (and had no way of knowing) that Plaintiffs' Private Information was unlawfully accessed and exfiltrated because Defendant kept this information secret until it posted public notice of the hacking incident on or around May 22, 2023.

411. Through no fault or lack of diligence, Plaintiffs and members of the Class were deceived and could not reasonably discover Defendant's deception and unlawful conduct. Plaintiffs and members of the Class did not discover and did not know of any facts that would have caused a reasonable person to suspect that Defendant was acting unlawfully as alleged herein.

412. At all times, Defendant was under a continuous duty to disclose to Plaintiffs and

members of the Class the nature and impact of the Data Breach. However, Defendant knowingly, actively, affirmatively, and/or negligently concealed the nature and impact of the Data Breach until on or around May 22, 2023, *years* after Plaintiffs' and Class Members' Private Information had been compromised.

413. For these reasons, all applicable statutes of limitations have been tolled based on the discovery rule and Defendant's concealment, and Defendant is estopped from relying on any statutes of limitations in defense of this action.

CLASS ACTION ALLEGATIONS

414. Plaintiffs bring this action individually and on behalf of all other persons similarly situated, pursuant to Federal Rule of Civil Procedure 23(a), 23(b)(1), 23(b)(2), and 23(b)(3).

415. Plaintiffs seek to represent the Nationwide Class defined as follows:

> **The Nationwide Class**
> All U.S. residents whose Private Information was accessed in the Data Breach, including all those who received a Notice Letter from, or on behalf of, Apria (the "Class").

416. Additionally, Plaintiffs Herrera, Kamisher, Stroffolino, Reese, and Kramer seek to represent the following California Subclass, defined as:

> **The California Subclass**
> All California residents whose Private Information was accessed in the Data Breach, including all those who received a Notice Letter from, or on behalf of, Apria (the "California Subclass").

417. Similarly, Plaintiffs Smith, Bobbitt, and Nikolich seek to represent the following Illinois Subclass, defined as:

> **The Illinois Subclass**
> All Illinois residents whose Private Information was accessed in the Data Breach, including all those who received a Notice Letter from, or on behalf of, Apria (the "Illinois Subclass").

418. Similarly, Plaintiff Munoz seeks to represent the following New York Subclass, defined as:

The New York Subclass
All New York residents whose Private Information was accessed in the Data Breach, including all those who received a Notice Letter from, or on behalf of, Apria (the "New York Subclass").

419. Plaintiffs May and Bennett also seek to represent the following Missouri Subclass, defined as:

The Missouri Subclass
All Missouri residents whose Private Information was accessed in the Data Breach, including all those who received a Notice Letter from, or on behalf of, Apria (the "Missouri Subclass").

420. Plaintiff Cuyle additionally seeks to represent the following Washington Subclass, defined as:

The Washington Subclass
All Washington residents whose Private Information was accessed in the Data Breach, including all those who received a Notice Letter from, or on behalf of, Apria (the "Washington Subclass").

421. 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.

422. 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.

423. 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 Plaintiffs 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.[51]

424. Typicality: Plaintiffs' claims are typical of the claims of the members of the classes because all Class Members had their Private Information accessed in the Data Breach and were harmed as a result.

425. Adequacy: Plaintiffs will fairly and adequately protect the interests of the Classes. Plaintiffs have no interest antagonistic to those of the classes and are aligned with Class Members' interests because Plaintiffs were subject to the same Data Breach as Class Members and face similar threats due to the Data Breach as Class Members. Plaintiffs have also retained competent counsel with significant experience litigating complex class actions, including Data Breach cases involving multiple classes.

426. 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 Plaintiffs and Class Members a duty to implement and maintain reasonable security procedures and practices to protect their Private 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 Plaintiffs' and Class Members' Private Information;

d. Whether Defendant breached its duty to implement reasonable security systems to

[51] *See* https://apps.web.maine.gov/online/aeviewer/ME/40/bf218a4e-1ffd-4f14-a74d-3d34aec8d6c7.shtml (last accessed Oct. 20, 2023).

protect Plaintiffs' and Class Members' Private Information;

e. Whether Defendant's breach of its duty to implement reasonable security systems directly and/or proximately caused damages to Plaintiffs 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 Plaintiffs and other Class Members are entitled to credit monitoring and other injunctive relief;

i. Whether Defendant provided timely notice of the Data Breach to Plaintiffs 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.

427. 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' Private Information, as well as Defendant's failure to timely alert affected customers to the Data Breach.

428. 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.

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

COUNT I
Negligence
(On Behalf of Plaintiffs and the Class)

430. Plaintiffs restate and reallege all of the allegations stated above as if fully set forth herein.

431. Defendant requires its patients, including Plaintiffs and Class Members, to submit non-public Private Information in the ordinary course of providing its products and services.

432. Defendant gathered and stored Plaintiffs' and Class Members' Private Information Private Information as part of its business of soliciting its products and services to patients, which solicitations and services affect commerce.

433. Plaintiffs and Class Members entrusted Defendant with their Private Information with the understanding that Defendant would safeguard their information. As evidenced by its privacy statements and conduct, Defendant understood its obligation to reasonably safeguard the Private Information that it collected from Plaintiffs and Class Members.

434. Defendant had full knowledge of the sensitivity of the Private Information and the types of harm that Plaintiffs and Class Members could and would suffer if the Private Information were wrongfully disclosed.

435. By assuming the responsibility to collect and store this data, and in fact doing so, and sharing it and using it for commercial gain, Defendant had a duty of care to use reasonable means to secure and safeguard their computer property—and Class Members' Private

Information held within it—to prevent disclosure of the information, and to safeguard the information from theft. Defendant's duty included a responsibility to implement processes by which they 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.

436. Defendant was subject to an "independent duty," untethered to any contract between Defendant and Plaintiffs or the Class.

437. Defendant owed a duty of care to Plaintiffs and Class Members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that its systems and networks, and the personnel responsible for them, adequately protected the Private Information.

438. Defendant's duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendant and its patients. That special relationship arose because Plaintiffs and the Class entrusted Defendant with their confidential Private Information, a necessary part of being Defendant's patients.

439. Defendant also had a duty to exercise appropriate clearinghouse practices to remove former patients' Private Information it was no longer required to retain pursuant to regulations.

440. Further, Defendant had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

441. Additionally, Defendant's duty to use reasonable security measures under HIPAA required Defendant to "reasonably protect" confidential data from "any intentional or

unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 45 C.F.R. § 164.530(c)(l). Some or all of the healthcare and/or medical information at issue in this case constitutes "protected health information" within the meaning of HIPAA.

442. Defendant's duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendant is bound by industry standards to protect confidential Private Information.

443. Moreover, Defendant had a duty to promptly and adequately notify Plaintiffs and the Class of the Data Breach.

444. Defendant had and continues to have a duty to adequately disclose that Plaintiffs' and Class Members' Private Information within Defendant's possession might have been compromised, how it was compromised, and precisely the types of data that were compromised and when. Such notice was necessary to allow Plaintiffs and the Class to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their Private Information by third parties.

445. Defendant breached its duties, pursuant to the FTC Act, HIPAA, other applicable standards and duties independent from statutes, and thus were negligent, by failing to use reasonable measures to protect Plaintiffs' and Class Members' Private Information. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' Private Information;

b. Failing to adequately monitor the security of their networks and systems;

c. Failing to periodically ensure that their email system had plans in place to maintain reasonable data security safeguards;

d. Allowing unauthorized access to Class Members' Private Information;

e. Failing to detect in a timely manner that Class Members' Private Information had been compromised;

f. Failing to encrypt the Private Information it maintained on its computer systems;

g. Failing to remove former patients' Private Information that it was no longer required to retain pursuant to regulations;

h. Failing to timely and adequately notify Class Members about the Data Breach's occurrence and scope, so that they could take appropriate steps to mitigate the potential for identity theft and other damages; and

i. Failing to secure its stand-alone personal computers, such as the reception desk computers, even after discovery of the data breach.

446. As a skilled entity in the healthcare field that possesses the sensitive Private Information of its current and former patients, Defendant owed a duty of care in protecting Plaintiffs' and Class Members' Private Information, pursuant to Section 5 of the FTC Act, HIPAA, and an independent duty of care.

447. In its Privacy Policy and HIPAA Privacy Notice (collectively, the "Privacy Policy"), Apria promises its patients that any disclosures of its patients' Private Information falling outside of the excepted circumstances set forth therein would be done "only with your written authorization."[52] However, Plaintiffs' and Class Members' Private Information has been

[52] *See* https://www.apria.com/hubfs/GEN-4539_Form_Notice-Privacy-Practices_04-22_v2_FNL.pdf (last visited on October 30, 2023).

disclosed without their written authorization as a result of the Data Breach.

448. Through its Privacy Policy, and in light of the highly sensitive and personal nature of the information Apria acquires and stores with respect to its patients, Apria promises to, among other things: keep patients' Private Information private; comply with industry standards related to data security and the maintenance of its patients' Private Information; inform its patients of its legal duties relating to data security and comply with all federal and state laws protecting patients' Private Information; only use and release patients' Private Information for reasons that relate to the services it provides; and provide adequate notice to patients if their Private Information is disclosed without authorization.

449. As evidenced by the occurrence of the Data Breach, Defendant negligently misrepresented its data security measures, Privacy Policy, and HIPAA Privacy Notice to Plaintiffs and Class Members.

450. As a skilled entity in the healthcare industry, Defendant violated Section 5 of the FTC Act and HIPAA by negligently misrepresenting its data security practices to Plaintiffs and Class Members.

451. As a skilled entity in the healthcare industry, Defendant violated Section 5 of the FTC Act and HIPAA by breaching its duties of care to Plaintiffs and Class Members, as provided in its Privacy Policy and HIPAA Privacy Notice.

452. Defendant further violated Section 5 of the FTC Act and HIPAA by failing to use reasonable measures to protect Private Information and not complying with applicable industry standards, as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of Private Information it obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiffs and the Class.

453. Plaintiffs and the Class are within the class of persons that the FTC Act and HIPAA were intended to protect.

454. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act and HIPAA were intended to guard against.

455. Defendant's violation of Section 5 of the FTC Act, HIPAA, and other duties (listed above) constitutes negligence.

456. 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 Plaintiffs and the Class.

457. A breach of security, unauthorized access, and resulting injury to Plaintiffs and the Class was reasonably foreseeable, particularly in light of Defendant's inadequate security practices.

458. It was foreseeable that Defendant's failure to use reasonable measures to protect Plaintiffs' and Class Members' Private Information would result in injury to Class Members. Further, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches in both the healthcare industry.

459. Defendant has full knowledge of the sensitivity of the Private Information and the types of harm that Plaintiffs and the Class could and would suffer if the Private Information were wrongfully disclosed.

460. Plaintiffs and the Class were the foreseeable and probable victims of any inadequate security practices and procedures. Defendant knew or should have known of the inherent risks in collecting and storing Plaintiffs' and Class Members' Private Information, the critical importance of providing adequate security of that Private Information, and the necessity

for encrypting Private Information stored on Defendant's systems.

461. It was therefore foreseeable that the failure to adequately safeguard Plaintiffs' and Class Members' Private Information would result in one or more types of injuries to Class Members.

462. Plaintiffs and the Class had no ability to protect their Private Information that was in, and possibly remains in, Defendant's possession.

463. Defendant was in a position to protect against the harm suffered by Plaintiffs and the Class as a result of the Data Breach.

464. Defendant's duty extended to protecting Plaintiffs and the Class from the risk of foreseeable criminal conduct of third parties, which has been recognized in situations where the actor's own conduct or misconduct exposes another to the risk or defeats protections put in place to guard against the risk, or where the parties are in a special relationship. *See* Restatement (Second) of Torts § 302B. Numerous courts and legislatures have also recognized the existence of a specific duty to reasonably safeguard personal information.

465. Defendant has admitted that the Plaintiffs' and Class Members' Private Information was wrongfully lost and disclosed to unauthorized third persons as a result of the Data Breach.

466. But for Defendant's wrongful and negligent breach of duties owed to Plaintiffs and the Class, their Private Information would not have been compromised.

467. There is a close causal connection between Defendant's failure to implement security measures to protect Plaintiffs' and Class Members' Private Information and the harm, or risk of imminent harm, suffered by Plaintiffs and the Class. Plaintiffs' and Class Members' Private Information was lost and accessed as the proximate result of Defendant's failure to

exercise reasonable care in safeguarding such Private Information by adopting, implementing, and maintaining appropriate security measures.

468. As a direct and proximate result of Defendant's negligence, Plaintiffs and the Class have suffered and will suffer injury, including but not limited to: (i) invasion of privacy; (ii) lost or diminished value of Private Information; (iii) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time; (iv) loss of benefit of the bargain; and (v) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remain backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information.

469. As a direct and proximate result of Defendant's negligence, the products and/or services that Defendant provided to Plaintiffs and Class Members damaged other property, including the value of their Private Information.

470. As a direct and proximate result of Defendant's negligence, Plaintiffs and the Class have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and noneconomic losses.

471. Additionally, as a direct and proximate result of Defendant's negligence, Plaintiffs and the Class have suffered and will suffer the continued risks of exposure of their Private Information, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information in its continued possession.

472. Plaintiffs and Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

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

474. Plaintiffs and Class Members are also entitled to injunctive relief requiring Defendant to (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) continue to provide adequate credit monitoring to all Class Members.

COUNT II
Negligence *Per Se*
(On Behalf of Plaintiffs and the Class)

475. Plaintiffs restate and reallege all of the allegations stated above as if fully set forth herein.

476. 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 Private Information. Various FTC publications and orders also form the basis of Defendant's duty.

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

478. Defendant's duty to use reasonable security measures under HIPAA required Defendant to "reasonably protect" confidential data from "any intentional or unintentional use or

disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 45 C.F.R. § 164.530(c)(l). Some or all of the healthcare and/or medical information at issue in this case constitutes "protected health information" within the meaning of HIPAA.

479. As a skilled entity in the healthcare industry that possesses the sensitive Private Information of its current and former patients, Defendant owed a duty of care in protecting Plaintiffs' and Class Members' Private Information, pursuant to Section 5 of the FTC Act, HIPAA, and an independent duty of care.

480. In its Privacy Policy and HIPAA Privacy Notice (collectively, the "Privacy Policy"), Apria promises its patients that any disclosures of its patients' Private Information falling outside of the excepted circumstances set forth therein would be done "only with your written authorization."[53] However, Plaintiffs' and Class Members' Private Information has been disclosed without their written authorization as a result of the Data Breach.

481. Through its Privacy Policy, and in light of the highly sensitive and personal nature of the information Apria acquires and stores with respect to its patients, Apria promises to, among other things: keep patients' Private Information private; comply with industry standards related to data security and the maintenance of its patients' Private Information; inform its patients of its legal duties relating to data security and comply with all federal and state laws protecting patients' Private Information; only use and release patients' Private Information for reasons that relate to the services it provides; and provide adequate notice to patients if their Private Information is disclosed without authorization.

---

[53] *See* https://www.apria.com/hubfs/GEN-4539_Form_Notice-Privacy-Practices_04-22_v2_FNL.pdf (last visited May 30, 2023).

482. As evidenced by the occurrence of the Data Breach, Defendant negligently misrepresented its data security measures, Privacy Policy, and HIPAA Privacy Notice to Plaintiffs and Class Members.

483. As a skilled entity, Defendant violated Section 5 of the FTC Act and HIPAA by negligently misrepresenting its data security practices to Plaintiffs and Class Members.

484. As a skilled entity, Defendant violated Section 5 of the FTC Act and HIPAA by breaching its duties of care to Plaintiffs and Class Members, as provided in its Privacy Policy and HIPAA Privacy Notice.

485. Defendant further violated Section 5 of the FTC Act and HIPAA by failing to use reasonable measures to protect Private Information and not complying with applicable industry standards, as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of Private Information it obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiffs and the Class.

486. Defendant's violation of Section 5 of the FTC Act, HIPAA, and other duties (listed above) constitutes negligence *per se*.

487. Class Members are consumers within the class of persons Section 5 of the FTC Act and HIPAA (and similar state statutes) were intended to protect.

488. Moreover, the harm that has occurred is the type of harm the FTC Act and HIPAA (and similar state statutes) were intended to guard against. Indeed, the FTC has pursued over fifty enforcement actions against healthcare entities 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 Plaintiffs and Class Members.

489. But for Defendant's wrongful and negligent breach of duties owed to Plaintiffs

and the Class, the Private Information of Plaintiffs and the Class would not have been compromised.

490. There is a close causal connection between Defendant's failure to implement security measures to protect Plaintiffs' and Class Members' Private Information and the harm, or risk of imminent harm, suffered by Plaintiffs and the Class. Plaintiffs' and Class Members' Private Information was lost and accessed as the proximate result of Defendant's failure to exercise reasonable care in safeguarding such Private Information by adopting, implementing, and maintaining appropriate security measures.

491. As a direct and proximate result of Defendant's negligence *per se*, Plaintiffs and the Class have suffered and will suffer injury, including but not limited to: (i) invasion of privacy; (ii) lost or diminished value of Private Information; (iii) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time; (iv) loss of benefit of the bargain; and (v) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remain backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information.

492. As a direct and proximate result of Defendant's negligence *per se*, Plaintiffs and the Class have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and noneconomic losses.

493. As a direct and proximate result of Defendant's negligence *per se*, the products and/or services that Defendant provided to Plaintiffs and Class Members damaged other property,

including the value of their Private Information.

494. Additionally, as a direct and proximate result of Defendant's negligence *per se*, Plaintiffs and the Class have suffered and will suffer the continued risks of exposure of their Private Information, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information in its continued possession.

495. Plaintiffs and Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

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

497. Plaintiffs and Class Members are also entitled to injunctive relief requiring Defendant to (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) continue to provide adequate credit monitoring to all Class Members.

COUNT III
Negligent Training and Supervision
(On Behalf of Plaintiffs and the Class)

498. Plaintiffs restate and reallege the allegations in all other paragraphs of this Consolidated Amended Complaint as if fully set forth herein.

499. At all times relevant hereto, Defendant owed a duty to Plaintiffs and Class Members to hire competent employees and agents, and to train and supervise them to ensure their recognition of the duties owed to their patients.

500. Defendant breached its duty to Plaintiffs and Class Members by failing to properly train and supervise its employees and agents who gave or allowed access to patient

medical records to one or more unauthorized users.

501. Defendant is also, or in the alternative, liable for the negligent acts of its employees and agents within the scope of their employment or agency under the doctrine of *respondeat superior*.

502. As a direct and proximate result of Defendant's breach of its duty of confidentiality and privacy and the disclosure of Plaintiffs' and Class Members' confidential medical information, Plaintiffs and Class Members suffered damages, including, without limitation, loss of the benefit of the bargain, exposure to heightened future risk of identity theft, loss of privacy, loss of confidentiality, embarrassment, emotional distress, humiliation and loss of enjoyment of life.

503. Plaintiffs and Class Members suffered and will continue to suffer damages including, but not limited to: (i) the untimely and/or inadequate notification of the Data Breach; (ii) improper disclosure of their PHI and PII; (iii) loss of privacy; (iv) out-of-pocket expenses incurred to mitigate the increased risk of identity theft and/or identity fraud caused by the Breach; (v) the value of their time spent mitigating identity theft and/or identity fraud and/or the increased risk of identity theft and/or identity fraud; (vi) the increased risk of identity theft; and, (vii) emotional distress. At the very least, Plaintiffs and Class Members are entitled to nominal damages.

504. Defendant's wrongful actions and/or inactions and the resulting Data Breach constituted (and continue to constitute) an invasion of Plaintiffs' and Class Members' privacy by publicly and wrongfully disclosing their private facts (i.e., their PHI and PII) without their authorization or consent.

COUNT IV
Breach of Contract
(On Behalf of Plaintiffs and the Class)

505. Plaintiffs restate and reallege all of the allegations stated above as if fully set forth herein.

506. Plaintiffs and Class Members entered into a valid and enforceable contract through which money was paid to Apria by them (or on their behalf) in exchange for goods and/or services. That contract included promises by Defendant to secure, safeguard, and not disclose Plaintiffs' and Class Members' Private Information.

507. Apria's Privacy Policy memorialized the rights and obligations of Apria and its patients. This document was provided to Plaintiffs and Class Members in a manner in which it became part of the agreement for services.

508. In the Privacy Policy, Apria commits to protecting the privacy and security of private information and promises to never share Plaintiffs' and Class Members' Private Information except under certain limited circumstances.

509. Plaintiffs and Class Members fully performed their obligations under their contracts with Apria.

510. However, Apria did not secure, safeguard, and/or keep private Plaintiffs' and Class Members' Private Information, and therefore Apria breached its contracts with Plaintiffs and Class Members.

511. Apria allowed third parties to access, copy, and/or exfiltrate Plaintiffs' and Class Members' Private information without permission. Therefore, Apria breached the Privacy Policy and consequently, its contract, with Plaintiffs and Class Members.

512. Apria's failure to satisfy its confidentiality and privacy obligations, specifically

those arising under the FTCA, HIPAA, and applicable industry standards, resulted in Apria providing services to Plaintiffs and Class Members that were of a diminished value.

513. As a result, Plaintiffs and Class Members have been harmed, damaged, and/or injured as described herein, including through Defendant's failure to fully perform its part of the bargain with Plaintiffs and Class Members.

514. As a direct and proximate result of Apria's conduct, Plaintiffs and Class Members suffered and will continue to suffer damages in an amount to be proven at trial.

515. In addition to monetary relief, Plaintiffs and Class Members are entitled to injunctive relief requesting 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 Plaintiffs and Class Members.

COUNT V
Breach of Implied Contract
(On Behalf of Plaintiffs and the Class)

516. Plaintiffs restate and reallege all of the allegations stated above as if fully set forth herein.

517. This Count is pleaded in the alternative to the breach of contact claim (Count IV) above.

518. Apria provides sleep apnea and other breathing care and treatment, wound care, diabetes equipment, and pharmaceutical services to its patients. Plaintiffs and Class Members formed an implied contract with Defendant regarding the provision of those goods and services through their collective conduct, including through payments made by Plaintiffs and Class Members or on their behalf for goods and services from Defendant.

519. Through Defendant's sale of goods and services to Plaintiffs and Class

Members, it knew or should have known that it must protect their confidential Private Information in accordance with its policies, practices, and applicable law and industry standards.

520. As consideration, (a) money was paid by Plaintiffs and Class Members (or on their behalf) to Apria, and (b) Plaintiffs and Class Members turned over valuable Private Information to Apria and allowed it to maintain and use their Private Information. Accordingly, Plaintiffs and Class Members bargained with Apria to securely maintain and store their Private Information.

521. Apria accepted the payments and took possession of Plaintiffs' and Class Members' Private Information for the purpose of providing goods and services to Plaintiffs and Class Members.

522. In delivering their Private Information to Apria and paying for goods and services, Plaintiffs and Class Members intended and understood that Apria would adequately safeguard the Private Information as part of the products and services being provided.

523. Defendant's implied promises to Plaintiffs and Class Members include, but are not limited to, (1) taking steps to ensure that anyone who is granted access to Private Information also protect the confidentiality of that data; (2) taking steps to ensure that the Private Information that is placed in its control is restricted and limited to achieve an authorized business purpose; (3) restricting access to qualified and trained employees and/or agents; (4) designing and implementing appropriate retention policies to protect the Private Information against criminal data breaches; (5) applying or requiring proper encryption; (6) implementing multifactor authentication for access; (7) complying with HIPAA and FTC standards to make sure that Plaintiffs' and Class Members' PHI would remain protected; and (8) taking other steps to protect against foreseeable data breaches.

524. Plaintiffs and Class Members would not have entrusted their Private Information to Apria in the absence of such an implied contract.

525. Had Apria disclosed to Plaintiffs and the Class that they did not have adequate computer systems and data security practices to secure their sensitive Private Information, Plaintiffs and Class Members would not have provided their Private Information to Apria.

526. As a provider of healthcare related products and services, Apria recognized or should have recognized that Plaintiffs' and Class Member's Private Information is highly sensitive and must be protected, and that this protection was of material importance as part of the bargain with Plaintiffs and the other Class Members.

527. Apria violated these implied contracts by failing to employ reasonable and adequate security measures to secure Plaintiffs' and Class Members' Private Information. Apria further breached these implied contracts by failing to comply with its promise to abide by HIPAA.

528. Additionally, Apria breached the implied contracts with Plaintiffs and Class Members by failing to ensure the confidentiality and integrity of electronic protected health information it created, received, maintained, and transmitted, in violation of 45 CFR 164.306(a)(1).

529. Apria also breached its implied contracts with Plaintiffs and Class Members by failing to implement technical policies and procedures for electronic systems that maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights, in violation of 45 CFR 164.312(a)(1).

530. Apria further breached the implied contracts with Plaintiffs and Class Members by failing to implement policies and procedures to prevent, detect, contain, and correct security violations, in violation of 45 CFR 164.308(a)(1).

531. Apria further breached the implied contracts with Plaintiffs and Class Members by failing to identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity, in violation of 45 CFR 164.308(a)(6)(ii).

532. Apria further breached the implied contracts with Plaintiffs and Class Members by failing to protect against any reasonably anticipated threats or hazards to the security or integrity of electronic protected health information, in violation of 45 CFR 164.306(a)(2).

533. Apria further breached the implied contracts with Plaintiffs and Class Members by failing to protect against any reasonably anticipated uses or disclosures of electronic protected health information that are not permitted under the privacy rules regarding individually identifiable health information, in violation of 45 CFR 164.306(a)(3).

534. Apria further breached the implied contracts with Plaintiffs and Class Members by failing to ensure compliance with the HIPAA security standard rules by its workforce violations, in violation of 45 CFR 164.306(a)(94).

535. Apria further breached the implied contracts with Plaintiffs and Class Members by impermissibly and improperly using and disclosing protected health information that is and remains accessible to unauthorized persons, in violation of 45 CFR 164.502, *et seq.*

536. Apria further breached the implied contracts with Plaintiffs and Class Members by failing to design, implement, and enforce policies and procedures establishing physical administrative safeguards to reasonably safeguard protected health information, in violation of 45 CFR 164.530(c).

537. Apria further breached the implied contracts with Plaintiffs and Class Members by otherwise failing to safeguard Plaintiffs' and Class Members' Private Information.

538. A meeting of the minds occurred, as Plaintiffs and Class Members agreed, *inter alia*, to provide their accurate, complete, and valuable Private Information and to pay Apria in exchange for Apria's agreement to, *inter alia*, protect their Private Information.

539. Plaintiffs and Class Members have been damaged by Apria's conduct, including the harms and injuries arising from the Data Breach now and in the future, as alleged herein.

COUNT VI
Bailment
(On Behalf of Plaintiffs and the Class)

540. Plaintiffs incorporate by reference those paragraphs set out above as if fully set forth herein.

541. Plaintiffs and the class delivered their Private Information to Defendant for the exclusive purpose of obtaining services. This data is valuable personal property belonging to Plaintiffs and the class members.

542. In delivering their personal property to Defendant, Plaintiffs and class members intended and understood that Defendant would adequately safeguard this property.

543. Defendant accepted possession of Plaintiffs' and class members' personal property for the purpose of providing services to Plaintiffs and class members.

544. By accepting possession of Plaintiffs' and class members' personal property, Defendant understood that Plaintiffs and class members expected Defendant to adequately safeguard this property. Accordingly, a bailment (or deposit) was established for the mutual benefit of the parties.

545. After accepting delivery of Plaintiffs' and class members' Private Information, Defendant maintained this intangible property within its exclusive possession. Plaintiffs and class members were unable to manipulate their personal data on Defendant's servers; Defendant was

in full control.

546. During the bailment (or deposit), Defendant owed a duty to Plaintiffs and class members to exercise reasonable care, diligence, and prudence in protecting their Private Information.

547. Defendant breached its duty of care by failing to take appropriate measures to safeguard and protect Plaintiffs' and class members' intangible property, resulting in the unlawful and unauthorized access to and misuse of Plaintiffs' and class members' Private Information.

548. As a proximate result of Defendant's failure to adequately protect the intangible personal property in its possession, Plaintiffs and the other class members have suffered, and will continue to suffer, damages in an amount to be proven at trial. In the alternative to compensatory damages, Plaintiffs and class members are entitled to nominal damages.

COUNT VII
Breach of Fiduciary Duty
(On Behalf of Plaintiffs and the Class)

549. Plaintiffs restate and reallege all of the allegations stated above as if fully set forth herein.

550. Defendant marketed and held themselves out to Plaintiffs and the community as experts in healthcare services and, thereafter, entered into a confidential hospital patient relationship with Plaintiffs and Class Members.

551. As part of the hospital patient relationship, Plaintiffs entrusted Defendant with their Private Information and relied upon Defendant to provide adequate and standardized data security to protect and preserve the confidentiality of their Private Information. Defendant accepted Plaintiffs' and Class Members' Private Information and trust as part of the relationship with the intent to provide healthcare services to Plaintiffs and Class Members.

552. Indeed, Defendant was in exclusive control of Patients' and Class Members Private Information that was held on its systems. This imbalance of superiority, confidence, and hospital patient relationship between the parties created a fiduciary relationship between Plaintiffs, the Class and Defendant.

553. In light of the fiduciary relationship between Defendant and Plaintiffs and Class Members, Defendant became a guardian of Plaintiffs' and Class Members' Private Information.

554. At all times, Defendant had a fiduciary duty to act for the benefit of Plaintiffs and Class Members upon matters within the scope of the fiduciary relationship. The fiduciary duties that arose included: (1) duties to design and implement adequate data security to safeguard Plaintiffs' and Class Members' Private Information; (2) duties to maintain the confidentiality of the Private Information it was entrusted; and (3) duties to notify Plaintiffs and Class Members of a data breach and disclose to the material facts of the Data Breach.

555. Defendant breached its fiduciary duties to Plaintiffs and Class Members by failing to adequately protect Plaintiffs' and Class Members' Private Information against cybersecurity events.

556. Defendant further breached its fiduciary duties by failing to notify, disclose, or inform Plaintiffs and Class Members of all material facts that related to the data breach, including the concealment of the root cause and the extent of exfiltration and theft of the Private Information.

557. Upon information and belief, Defendant breached its fiduciary duties to Plaintiffs and Class Members by:

a. failing to encrypt and otherwise protect the integrity of the IT systems containing Plaintiffs' and Class Members' Private Information;

b. failing to ensure the confidentiality and integrity of electronic PHI Defendant

created, received, maintained, and transmitted, in violation of 45 C.F.R. § 164.306(a)(1);

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

d. failing to implement policies and procedures to prevent, detect, contain, and correct security violations, in violation of 45 C.F.R. § 164.308(a)(1);

e. failing to identify and respond to suspected or known security incidents and to mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity in violation of 45 C.F.R. § 164.308(a)(6)(ii);

f. failing to protect against any reasonably-anticipated threats or hazards to the security or integrity of electronic PHI in violation of 45 C.F.R. § 164.306(a);

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

h. failing to ensure compliance with the HIPAA security standard rules by its workforce in violation of 45 C.F.R. § 164.306(a)(94);

i. impermissibly and improperly using and disclosing PHI that is and remains accessible to unauthorized persons in violation of 45 C.F.R. § 164.502, *et seq.*

j. failing to effectively train all members of its workforce (including independent contractors) on the policies and procedures with respect to PHI as necessary and appropriate for the members of its workforce to carry out their functions and to

maintain security of PHI in violation of 45 C.F.R. § 164.530(b) and 45 C.F.R. § 164.308(a)(5);

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

l. otherwise failing to safeguard Plaintiffs' and Class Members' Private Information.

558. As a direct and proximate result of Defendant's breach of its fiduciary duties, the data breach occurred and Plaintiffs and Class Members have and will suffer actual, consequential, loss of benefit of the bargain, and nominal damages, where actual damages cannot be proven.

559. Plaintiffs are further entitled to injunctive relief requiring defendant to: (1) fully disclose the mechanics and root cause of the Data Breach, (2) fully disclose the extent of compromise and exfiltration of the Private Information, (3) fully disclose all remedial measures taken post data breach, and (4) to implement and provide additional data security safeguards to protect the Private Information that remains in its possession and at risk of future compromise.

COUNT VIII
Breach of Confidence
(On Behalf of Plaintiffs and the Class)

560. Plaintiffs restate and reallege all of the allegations stated above as if fully set forth herein.

561. At all times during Plaintiffs' and Class Members' interactions with Defendant, Defendant was fully aware of the confidential and sensitive nature of Plaintiffs' and Class Members' Private Information that Plaintiffs and Class Members provided to Defendant.

562. Defendant's relationship with Plaintiffs and Class Members was governed by terms and expectations that Plaintiffs' and Class Members' Private Information would be

collected, stored, and protected in confidence, and would not be disclosed to unauthorized third parties.

563. Plaintiffs and Class Members provided their Private Information to Defendant with explicit and implicit understandings that Defendant would protect and not permit the Private Information to be disseminated to any unauthorized third parties.

564. Plaintiffs and Class Members provided their Private Information to Defendant with the explicit and implicit understandings that Defendant would take precautions to protect that Private Information from unauthorized disclosure.

565. Defendant voluntarily received in confidence Plaintiffs' and Class Members' Private Information with the understanding that Private Information would not be disclosed or disseminated to unauthorized third parties or to the public.

566. Due to Defendant's failure to prevent and avoid the Data Breach from occurring, Plaintiffs' and Class Members' Private Information was disclosed and misappropriated to unauthorized third parties beyond Plaintiffs' and Class Members' confidence, and without their express permission.

567. As a proximate result of such unauthorized disclosures, Plaintiffs and Class Members suffered damage.

568. But for Defendant's disclosure of Plaintiffs' and Class Members' Private Information in violation of the parties' understanding of confidence, their Private Information would not have been compromised, stolen, viewed, accessed, and/or used by unauthorized third parties.

569. The injury and harm suffered by Plaintiffs and Class Members was the reasonably foreseeable result of Defendant's inadequate security of Plaintiffs' and Class Members' Private

Information. Defendant knew or should have known that their methods of accepting, storing, transmitting, and using Plaintiffs' and Class Members' Private Information was inadequate.

570. As a direct and proximate result of Defendant's negligent conduct, Plaintiffs and Class Members have suffered injury, including but not limited to (1) threat of identity theft; (2) the loss of the opportunity of how their Private Information is used; (3) the compromise, publication, and/or theft of their Private Information; (4) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their Private Information; (5) the continued risk to their Private Information, which may remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiffs' and Class Members' Private Information and its continued possession; and (6) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the Private Information compromised a s result of the Data Breach for the remainder of the lives of Plaintiffs and Class Members.

571. As a direct and proximate result of such unauthorized disclosures, Plaintiffs and Class Members have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

COUNT IX
Conversion
(On Behalf of Plaintiffs and the Class)

572. Plaintiffs restate and reallege the allegations in all other paragraphs of this Consolidated Amended Complaint as if fully set forth herein.

573. Defendant exerted control over Plaintiffs' and Class Members' personal property

(i.e., the Private Information).

574. Defendant exerted unauthorized control over Private Information belonging to Plaintiffs and Class Members by sharing or disclosing Private Information to third parties.

575. Defendant knowingly exerted unauthorized control over Plaintiffs' and Class Members' Private Information because Defendant was aware of a high probability that it was disclosing Private Information to third parties in the Data Breach.

576. Defendant committed criminal conversion as defined by Indiana Code § 35-43-4-3.

577. Plaintiffs and Class Members have suffered, and are suffering, pecuniary losses as a result of Defendant's violation of Indiana Code § 35-43-4-3.

578. Plaintiff and Class Members are entitled to recover an amount not to exceed three times their actual damages, the costs of the action, reasonable attorneys' fees, travel expenses, loss of time related to the recovery of a judgment, direct and indirect expenses, and all other reasonable costs of collection. Ind. Code § 34-24-3-1.

COUNT X
Invasion of Privacy – Intrusion Upon Seclusion
(On Behalf of Plaintiffs and the Class)

579. Plaintiffs restate and reallege all of the allegations stated above as if fully set forth herein.

580. Indiana recognizes the tort of invasion of privacy by intrusion upon seclusion.

581. Plaintiffs and the Class had a legitimate expectation of privacy to their PII and were entitled to the protection of this information against disclosure to unauthorized third parties.

582. Defendant owed a duty to Plaintiffs and the Class Members, to keep their PII confidential.

583. Defendant failed to protect said PII and exposed the PII of Plaintiffs and the Class Members to unauthorized persons, which is now publicly available, and on information and belief, on the dark web, and subject to fraudulent misuse.

584. Defendant allowed unauthorized third parties access to and examination of the PII of Plaintiffs and the Class Members, by way of Defendant's failure to protect the PII.

585. The unauthorized release to, custody of, and examination by unauthorized third parties of the PII of Plaintiffs and the Class Members is highly offensive to a reasonable person.

586. The intrusion was into a place or thing, which was private and is entitled to be private. Plaintiffs' and the Class Members' PII was disclosed to Defendant in connection with the receipt of healthcare services with Defendant, but privately with an intention that the PII would be kept confidential and would be protected from unauthorized disclosure. Plaintiffs and the Class Members were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization.

587. The Data Breach constitutes an intentional or reckless, and substantial, interference by Defendant with Plaintiffs' and the Class Members' interests in solitude or seclusion, either as to their persons or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

588. Defendant acted with a knowing state of mind when it permitted the Data Breach to occur because it had actual knowledge that its data security practices were inadequate and insufficient.

589. Defendant acted with reckless disregard for Plaintiffs' and Class Members' privacy when they allowed improper access to its systems containing Plaintiffs' and Class Members' Private Information.

590. Defendant was aware of the potential of a data breach and failed to adequately safeguard its systems and implement appropriate policies to prevent the unauthorized release of Plaintiffs' and Class Members' Private Information.

591. Because Defendant acted with this knowing state of mind, it had notice and knew the inadequate and insufficient information security practices would cause injury and harm to Plaintiffs and the Class Members.

592. As a direct and proximate result of Defendant's invasion of privacy, intrusion upon seclusion, set forth in the preceding paragraphs, Plaintiffs and Class Members have suffered or will imminently suffer injury and damages as set forth herein, including fraudulent misuse of their PII; loss of the opportunity to control how their PII is used; diminution in value of their PII; compromise and continuing publication of their PII; and the value of time and labor expended to mitigate the consequences of the Data Breach, and are entitled to compensatory, actual, and punitive damages as a result.

593. Plaintiffs and Class Members are also entitled to injunctive relief requiring Defendant to (i) strengthen their data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) continue to provide adequate credit monitoring to all Class Members.

594. Unless and until enjoined, and restrained by order of this Court, Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiffs and the Class Members in that the PII maintained by Defendant can be viewed, distributed, and used by unauthorized persons for years to come. Plaintiffs and the Class Members have no adequate remedy at law for the injuries in that a judgment for monetary damages will not end the invasion of privacy for Plaintiffs and the Class Members.

COUNT XI
Invasion of Privacy – Public Disclosure of Private Facts
(On Behalf of Plaintiffs and the Class)

595. Plaintiffs restate and reallege all of the allegations stated above as if fully set forth herein.

596. Indiana recognizes the tort of invasion of privacy by public disclosure of private facts.

597. Plaintiffs and the Class had a legitimate expectation of privacy to their Private Information and were entitled to the protection of this information against disclosure to unauthorized third parties.

598. Defendant owed a duty to Plaintiffs and the Class Members, to keep their Private Information confidential.

599. Defendant failed to protect said Private Information and exposed the Private Information of Plaintiffs and the Class Members to unauthorized persons, which is now publicly available, and on information and belief, on the dark web, and subject to fraudulent misuse.

600. Defendant allowed unauthorized third parties access to and examination of the Private Information of Plaintiffs and the Class Members, by way of Defendant's failure to protect the Private Information.

601. The unauthorized release to, custody of, and examination by unauthorized third parties of the Private Information of Plaintiffs and the Class Members is highly offensive to a reasonable person.

602. The information disclosed was private and is entitled to be private. Plaintiffs' and the Class Members' Private Information was disclosed to Defendant in connection with receiving healthcare services from with Defendant, but privately with an intention that the Private

Information would be kept confidential and would be protected from unauthorized disclosure. Plaintiffs and the Class Members were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization.

603. Defendant acted with reckless disregard for Plaintiffs' and Class Members' privacy when they allowed improper access to its systems containing Plaintiffs' and Class Members' Private Information.

604. Defendant was aware of the potential of a data breach and failed to adequately safeguard its systems and implement appropriate policies to prevent the unauthorized release of Plaintiffs' and Class Members' Private Information.

605. Defendant disclosed Plaintiffs' and Class Members' Private Information in a manner or way that reaches the public in general or a large enough number of persons that the information is sure to become public knowledge, i.e., on the Dark Web.

606. As a direct and proximate result of Defendant's invasion of privacy, public disclosure, set forth in the preceding paragraphs, Plaintiffs and Class Members have suffered or will imminently suffer injury and damages as set forth herein, including fraudulent misuse of their Private Information; loss of the opportunity to control how their Private Information is used; diminution in value of their Private Information; compromise and continuing publication of their Private Information; and the value of time and labor expended to mitigate the consequences of the Data Breach, and are entitled to compensatory, actual, and punitive damages as a result.

607. Plaintiffs and Class Members are also entitled to injunctive relief requiring Defendant to (i) strengthen their data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) continue to provide adequate credit monitoring to all Class Members.

608. Unless and until enjoined, and restrained by order of this Court, Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiffs and the Class Members in that the Private Information maintained by Defendant can be viewed, distributed, and used by unauthorized persons for years to come. Plaintiffs and the Class Members have no adequate remedy at law for the injuries in that a judgment for monetary damages will not end the invasion of privacy for Plaintiffs and the Class Members.

COUNT XII
Unjust Enrichment
(On Behalf of Plaintiffs and the Class)

609. Plaintiffs restate and reallege all of the allegations stated above as if fully set forth herein.

610. This count is pleaded in the alternative to the Breach of Contract (Count III) and Breach of Implied Contract claim (Count IV) above.

611. Plaintiffs and Class Members conferred a monetary benefit on Defendant. Specifically, they paid for services and/or products from Defendant and/or its agents and in so doing also provided Defendant with their Private Information. In exchange, Plaintiffs and Class Members should have received from Defendant the services and/or products that were the subject of the transaction and should have had their Private Information protected with adequate data security.

612. Defendant knew that Plaintiffs and Class Members conferred a benefit on it in the form their Private Information as well as payments made on their behalf as a necessary part of their receiving products and/or services from Defendant. Defendant appreciated and accepted that benefit. Defendant profited from these transactions and used the Private Information of Plaintiffs and Class Members for business purposes.

613. Upon information and belief, Defendant funds its data security measures entirely from its general revenue, including payments on behalf of or for the benefit of Plaintiffs and Class Members.

614. As such, a portion of the payments made for the benefit of or on behalf of Plaintiffs and Class Members is to be used to provide a reasonable level of data security, and the amount of the portion of each payment made that is allocated to data security is known to Defendant.

615. Defendant, however, failed to secure Plaintiffs' and Class Members' Private Information and, therefore, did not provide adequate data security in return for the benefit Plaintiffs and Class Members provided.

616. Defendant would not be able to carry out an essential function of its regular business without the Private Information of Plaintiffs and Class Members and derived revenue by using it for business purposes. Plaintiffs and Class Members expected that Defendant or anyone in Defendant's position would use a portion of that revenue to fund adequate data security practices.

617. Defendant acquired the Private Information through inequitable means in that it failed to disclose the inadequate security practices previously alleged.

618. If Plaintiffs and Class Members knew that Defendant had not reasonably secured their Private Information, they would not have allowed their Private Information to be provided to Defendant.

619. When Plaintiffs and Class Members paid for services and provided their Private Information to Apria, they did so on the mutual understanding and expectation that Apria would use a portion of those payments, or revenue derived from the use of their Private Information, to adequately fund data security practices.

620. Upon information and belief, Apria funds their data security measures entirely

from their general revenues, including payments made by or on behalf of Plaintiffs and Class Members and revenue derived from the Private Information provided by Plaintiffs and Class Members.

621. As such, a portion of the payments made by or on behalf of Plaintiffs and Class Members, or the revenue derived from their Private Information, is to be used by Apria to provide a reasonable level of data security, and the amount of the portion of each payment made that is allocated to data security is known to Apria.

622. Apria enriched themselves by saving the costs they reasonably should have expended on data security measures to secure Plaintiffs' and Class Members' Private Information and instead directing those funds to their own profits. Instead of providing a reasonable level of security that would have prevented the hacking incident, Apria instead calculated to increase their own profits at the expense of Plaintiffs and Class Members by utilizing cheaper, ineffective security measures. Plaintiffs and Class Members, on the other hand, suffered as a direct and proximate result of Apria's decision to prioritize their own profits over the requisite security.

623. Apria knew that Plaintiffs and Class Members conferred a benefit which Apria accepted. Apria profited from these transactions and used the Private Information of Plaintiffs and Class Members for business purposes.

624. For years and continuing to today, Apria's business model has depended upon their use of consumers' Private Information. Trust and confidence are critical and central to the services provided by Apria in the health care industry. Unbeknownst to Plaintiffs and Class Members, however, Apria did not secure, safeguard, or protect its patients' data and employed deficient security procedures and protocols to prevent unauthorized access to patients' Private Information. Apria's deficiencies described herein were contrary to their security messaging.

625. Plaintiffs and Class Members received health care services and medical treatment from Apria, and Apria was provided with, and allowed to collect and store, their Private Information on the mistaken belief that Apria complied with their duties to safeguard and protect its patients' Private Information.

626. Upon information and belief, putting their short-term profit ahead of safeguarding Private Information, and unbeknownst to Plaintiffs and Class Members, Apria knowingly sacrificed data security to save money at their expense and to their detriment.

627. Upon information and belief, Apria knew that the manner in which they maintained and transmitted patient Private Information violated federal regulations, industry standards, and its fundamental duties owed to Plaintiffs and Class Members by neglecting well accepted security measures to ensure confidential information was not accessible to unauthorized access. Apria had knowledge of methods for designing safeguards against unauthorized access and eliminating the threat of exploitation, but it did not use such methods.

628. Apria had within their exclusive knowledge, and never disclosed, that they had failed to safeguard and protect Plaintiffs' and Class Members' Private Information. This information was not available to Plaintiffs, Class Members, or the public at large.

629. Apria also knew that Plaintiffs and Class Members expected security against known risks and that they were required to adhere to state and federal standards for the protection of confidential personally identifying, sensitive medical, and other personal information.

630. Plaintiffs and Class Members did not expect that Apria would knowingly insecurely maintain and hold their Private Information when that data was no longer needed to facilitate medical treatment, business, health care transactions, or other legitimate business reason. Likewise, Plaintiffs and Class Members did not know or expect that Apria would employ

substantially deficient data security systems and fail to undertake any required monitoring or supervision of the entrusted Private Information.

631. Had Plaintiffs and Class Members known about Apria's deficiencies and efforts to hide their ineffective and substandard data security systems, Plaintiffs and Class Members would not have sought medical treatment from Apria.

632. By withholding the facts concerning the defective security and protection of patient Private Information, Apria put their own interests ahead of the very patients who placed their trust and confidence in Apria and benefitted themselves to the detriment of Plaintiffs and Class Members.

633. It would be inequitable, unfair, and unjust for Apria to retain these wrongfully obtained fees and benefits. Apria's retention of wrongfully obtained monies would violate fundamental principles of justice, equity, and good conscience.

634. Plaintiffs and Class Members have no adequate remedy at law.

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

COUNT XIII
Violations of the Indiana Deceptive Consumer Sales Act,
Ind. Code § 24-5-0.5 *et seq.*
(On Behalf of Plaintiffs and the Class)

636. Plaintiffs restate and reallege all of the allegations stated above as if fully set forth herein.

637. Plaintiffs, Class Members and Defendant each qualify as parties engaging in consumer transactions, as defined in Ind. Code § 24-5-0.5-2(a)(1).

638. As alleged herein in this Complaint, Defendant engaged in unfair or deceptive acts or practices in the conduct of consumer transactions in violations of the DCSA, including but not limited to:

a. Representing that its services were of a particular standard or quality that it knew or should have known were of another;

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

c. Failing to identify foreseeable security and privacy risks, and remediate identified security and privacy risks, which was a direct and proximate cause of the Data Breach;

d. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Class Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Cyber-Attack and data breach;

e. Misrepresenting that it would protect the privacy and confidentiality of Plaintiffs' and Class Members' Private Information, including by implementing and maintaining reasonable security measures;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiffs' and Class Members' Private Information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Class Members' Personal Information, including duties imposed by

the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Security breach.

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

640. In addition, Defendant's failure to secure customers' Private Information violated the FTC Act and therefore violates the DCSA.

641. Defendant knew or should have known that its computer systems and data security practices were inadequate to safeguard the Private Information of Plaintiffs and Class Members, deter hackers, and detect a breach within a reasonable time, and that the risk of a data breach was highly likely.

642. The aforesaid conduct violated the DCSA, Ind. Code § 24-5-0.5 et seq., in that it is a restraint on trade or commerce.

643. The Defendant's violations of the DCSA have an impact of great and general importance to the public, including the people of Indiana. Thousands of Indiana residents have received services from Defendant, many of whom have been impacted by the Data Breach. In addition, Indiana residents have a strong interest in regulating the conduct of its health care services, whose policies described herein affect millions of people across the country.

644. As a direct and proximate result of Defendant's violation of the DCSA, Plaintiffs and Class Members are entitled to judgment under Ind. Code § 24-5-0.5, et seq., to enjoin further violations, to recover actual damages, to recover the costs of this action (including reasonable attorneys' fees), and such other further relief as the Court deems just and proper.

645. On information and belief, Defendant formulated and conceived of the systems it

used to compile and maintain customer information largely within the state of Indiana, oversaw its data privacy program complained herein from Indiana, and its communications and other efforts to hold customer data largely emanated from Indiana.

646. Most, if not all, of the alleged misrepresentations and omissions by Defendant that led to inadequate safety measures to consumer information occurred within or were approved within Indiana.

647. Defendant's implied and express representations that they would adequately safeguard Plaintiffs' and Class Members' Private Information constitute representations as to the particular standard, quality, or grade of services that such services did not actually have (as the data security services were of another, inferior quality), in violation of Ind. Code § 24-5-0.5, et seq.

648. These violations have caused financial injury to Plaintiffs and Class Members and created an unreasonable, imminent risk of future injury.

649. Accordingly, Plaintiffs, on behalf of themselves and Class Members, bring this action under the Deceptive Consumer Sales Act to seek such injunctive relief necessary to enjoin further violations and to recover costs of this action, including reasonable attorneys' fees and other costs.

COUNT XIV
Violations of California's Unfair Competition Act
Cal. Bus. & Prof. Code §§ 17200 *et seq.*
(On Behalf of Plaintiffs Herrera, Kamisher, Stroffolino, Reese, Kramer and the California Subclass)

650. Plaintiffs Herrera, Kamisher, Stroffolino, Reese, and Kramer (for the purposes of this count, "Plaintiffs") restate and reallege all of the allegations stated above as if fully set forth herein and bring this claim on behalf of themselves and the California Subclass.

651. Apria is a "person" as defined by Cal. Bus. & Prof. Code § 17201.

652. Apria violated Cal. Bus. & Prof. Code §§ 17200 et seq. (the "UCL") by engaging in unlawful, unfair, and deceptive business acts and practices, as set forth herein.

1. Apria's "unfair" acts and practices include:

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

b. Failing to identify foreseeable security risks, remediate identified security risks, and sufficiently improve security following previous cybersecurity incidents, as alleged herein. This conduct, with little if any utility, is unfair when weighed against the harm to Plaintiffs and California Subclass Members, whose Private Information has been compromised;

c. Failing to implement and maintain reasonable security measures, contrary to legislatively declared public policy that seeks to protect consumers' data and ensure that entities that are trusted with it use appropriate security measures. These policies are reflected in laws that include, but are not limited to, the FTC Act, 15 U.S.C. § 45, California's Consumer Records Act, Cal. Civ. Code § 1798.81.5, and California's Consumer Privacy Act, Cal. Civ. Code § 1798.100; and

d. Failing to implement and maintain reasonable data security measures, resulting in substantial consumer injuries, as alleged above, that are not outweighed by any countervailing benefits to consumers or competition. Moreover, because consumers could not have known of Apria's grossly inadequate security, they could not have

reasonably avoided the harms that Apria's lax data security standards and procedures caused.

653. Apria has also engaged in "unlawful" and "deceptive" business practices by violating multiple laws, including California's Consumer Records Act, Cal. Civ. Code §§ 1798.81.5 (requiring reasonable data security measures) and 1798.82 (requiring timely breach notification), California's Consumer Privacy Act, Cal. Civ. Code § 1798.100, California common law, and the FTC Act, 15 U.S.C. § 45.

654. Apria's "unlawful" and "deceptive" acts and practices include:

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

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

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and California Subclass Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;

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

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and California Subclass

Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45;

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

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and California Subclass Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, California's Consumer Privacy Act, Cal. Civ. Code § 1798.100, and California's Customer Records Act, Cal. Civ. Code §§ 1798.80 *et seq.,* and § 1798.81.5, which was a direct and proximate cause of the Data Breach; and

h. Failing to timely provide the Notice of Data Breach required by Cal. Civ. Code § 1798.82(d)(1).

655. Apria's representations and omissions were material because they were likely to deceive reasonable individuals about the adequacy of Apria's data security and ability to protect the confidentiality of their Private Information.

656. Plaintiffs and California Subclass Members would not have entrusted their Private Information to Defendant, or would not have used Defendant's services or products had they known that Defendant would fail to implement reasonable data security or fail to notify them following its discovery of the Data Breach.

657. As a direct and proximate result of Apria's unfair and unlawful acts and practices, Plaintiffs and California Subclass Members were injured and suffered monetary and non-monetary damages, as alleged herein, including but not limited to, actual misuse of their Private Information

resulting in fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their Private Information; overpayment for Apria's services; loss of the value of access to their Private Information; and the value of identity protection services made necessary by the Data Breach.

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

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

COUNT XV
Violations of the California Confidentiality of Medical Information Act
Cal. Civ. Code § 56, *et seq.*
(On Behalf of Plaintiffs Herrera, Kamisher, Stroffolino, Reese, Kramer and the California Subclass)

660. Plaintiffs Herrera, Kamisher, Stroffolino, Reese, and Kramer (for the purposes of this count, "Plaintiffs") restate and reallege all of the allegations stated above as if fully set forth herein and bring this claim on behalf of themselves and the California Subclass.

661. Defendant is a healthcare provider who is subject to the requirements and mandates of the California Confidentiality of Medical Information Act, Cal. Civ. Code § 56, et seq. ("CMIA").

662. California's Confidentiality of Medical Information Act ("CMIA") requires a

healthcare Provider "who creates, maintains, preserves, stores, abandons, destroys, or disposes of medical information [to] do so in a manner that preserves the confidentiality of the information contained therein." Cal. Civ. Code § 56.101. "Every provider of health care, health care service plan, pharmaceutical company, or contractor who negligently creates, maintains, preserves, stores, abandons, destroys, or disposes of medical information shall be subject to the remedies and penalties provided under subdivisions (b) and (c) of Section 56.36." Id.

663. Defendant is a "provider[s] of health care"; it is "organized for 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." Cal. Civ. Code § 56.06(a).

664. The CMIA requires that "[a]n electronic health record system or electronic medical record system . . . [p]rotect and preserve the integrity of electronic medical information." Cal. Civ. Code § 56.101(b)(1)(A).

665. Plaintiffs and California Subclass members are "patient[s]," "whether or not still living, who received health care services from a provider of health care and to whom medical information pertains" pursuant to § 56.05(k) of the CMIA.

666. The PHI of Plaintiffs and California Subclass members compromised in the Data Breach constitutes "medical information" maintained in electronic form pursuant to § 56.05(j) of the CMIA.

667. Defendant violated § 56.36(b) of the CMIA by negligently maintaining, preserving, storing and releasing the PHI of Plaintiffs and California Subclass members, and failing to protect and preserve the integrity of the PHI of Plaintiffs and California Subclass members. Plaintiffs and California Subclass members did not authorize Defendant's disclosure

and release of their PHI that occurred in the Data Breach.

668. As a result of the Data Breach, the PHI of Plaintiffs and California Subclass members was compromised when it was acquired and accessed by unauthorized parties.

669. Defendant violated the CMIA by negligently (1) failing to implement reasonable

670. administrative, physical and technical safeguards to protect, secure and prevent the unauthorized access to, and acquisition of, Plaintiffs' and California Subclass members' PHI; (2) failing to implement reasonable data security measures, such as intrusion detection processes that detect data breaches in a timely manner, to protect and secure Plaintiffs' and California Subclass members'

671. PHI; (3) failing to use reasonable authentication procedures to track PHI in case of a security breach; and (4) allowing undetected and unauthorized access to servers, networks and systems where Plaintiffs' and California Subclass members' PHI was kept, all in violation of the CMIA.

672. Defendant's failure to implement adequate data security measures to protect the PHI of Plaintiffs and California Subclass members was a substantial factor in allowing unauthorized parties to access Defendant's computer systems and acquire the PHI of Plaintiffs and California Subclass members.

673. As a direct and proximate result of Defendant's violation of the CMIA, Defendant allowed the PHI of Plaintiffs and California Subclass members to (a) escape and spread from its normal place of storage through unauthorized disclosure or release; and (b) be accessed and acquired by unauthorized parties in order to, on information and belief, view, mine, exploit, use, and /or profit from their PHI, thereby breaching the confidentiality of their PHI. Plaintiffs and California Subclass members have accordingly sustained and will continue to sustain actual

damages as set forth above.

674. Plaintiffs, individually and on behalf of California Subclass members, seeks actual and statutory damages pursuant to § 56.36(b)(1) of the CMIA.

675. As a direct and proximate result of Defendant's violations of the CMIA, Plaintiffs and California Subclass members have been injured within the meaning of the CMIA and are entitled to damages of $1,000 each pursuant to Cal. Civ. Code § 56.36(b)(1).

676. Plaintiffs also seeks reasonable attorneys' fees and costs under applicable law including Civil Code § 56.35 and California Code of Civil Procedure § 1021.5.

COUNT XVI
Violations of Illinois Consumer Fraud and Deceptive Business Practices Act ("CFA")
815 Ill. Comp. Stat. §§ 505/1, *et seq.*
(On Behalf of Plaintiffs Smith, Bobbitt, Nikolich and the Illinois Subclass)

677. Plaintiffs Smith, Bobbitt, and Nikolich (for the purposes of this count, "Plaintiffs") restate and reallege all of the allegations stated above as if fully set forth herein and bring this claim on behalf of themselves and the Illinois Subclass.

678. Plaintiffs and the Illinois Subclass are "consumers" as defined in 815 Ill. Comp. Stat. § 505/1(e). Plaintiffs, the Illinois Subclass, and Defendant are "persons" as defined in 815 Ill. Comp. Stat. § 505/1(c).

679. Defendant engaged in "trade" or "commerce," including the provision of services, as defined under 815 Ill. Comp. Stat. § 505/1(f). And pursuant to Defendant's "trade" or "commerce," Defendant disclosed Plaintiffs and Illinois Subclass Members' Private Information to its outside counsel. Moreover, Defendant engages in the sale of "merchandise" (including services) as defined by 815 Ill. Comp. Stat. § 505/1(b) and (d).

680. Defendant engaged in deceptive and unfair acts and practices, misrepresentation, and the concealment and omission of material facts in connection with the sale and advertisement

of their services in violation of the CFA, including: (i) failing to maintain and/or ensure that adequate data security was used—including by Defendant's outside counsel—as to keep Plaintiffs' and the Illinois Subclass Members' sensitive Private Information from being stolen by cybercriminals and failing to comply with applicable state and federal laws and industry standards pertaining to data security, including the FTC Act; (ii) failing to disclose or omitting materials facts to Plaintiffs and the Illinois Subclass regarding the lack of adequate data security and inability or unwillingness to properly secure and protect the Private Information of Plaintiffs and the Illinois Subclass; (iii) failing to disclose or omitting materials facts to Plaintiffs and the Illinois Subclass about Defendant's failure to comply with the requirements of relevant federal and state laws pertaining to the privacy and security of the Private Information of Plaintiffs and the Illinois Subclass; and (iv) failing to take proper action following the Data Breach to enact adequate privacy and security measures and protect Plaintiffs' and the Illinois Subclass's Private Information and other personal information from further unauthorized disclosure, release, data breaches, and theft.

681. These actions also constitute deceptive and unfair acts or practices because Defendant knew the facts about the inadequate data security and failure to comply with applicable state and federal laws and industry standards would be unknown to and not easily discoverable by Plaintiffs and the Illinois Subclass and defeat their reasonable expectations about the security of their Private Information.

682. Defendant intended that Plaintiffs and the Illinois Subclass rely on its deceptive and unfair acts and practices and the concealment and omission of material facts in connection with Defendant's offering of goods and services.

683. Defendant's wrongful practices were and are injurious to the public because those practices were part of Defendant's generalized course of conduct that applied to the Illinois

Subclass. Plaintiffs and the Illinois Subclass have been adversely affected by Defendant's conduct and the public was and is at risk as a result thereof.

684. Defendant also violated 815 ILCS 505/2 by failing to immediately notify Plaintiffs and the Illinois Subclass of the nature and extent of the Data Breach pursuant to the Illinois Personal Information Protection Act, 815 ILCS 530/1, *et seq*.

685. As a result of Defendant's wrongful conduct, Plaintiffs and the Illinois Subclass were injured in that they never would have provided their Private Information to Defendant, or purchased Defendant's services, had they known or been told that Defendant failed to maintain and/or ensure sufficient security as to keep their Private Information from being hacked and taken and misused by others.

686. As a direct and proximate result of Defendant's violations of the CFA, Plaintiffs and the Illinois Subclass have suffered harm: (i) actual identity theft; (ii) the loss of the opportunity how their Private Information is used; (iii) the compromise, publication, and/or theft of their Private Information; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their Private Information; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (vi) the continued risk to their Private Information, which remain in Defendant's possession and/or control and is subject to further unauthorized disclosures so long as Defendant fail to undertake appropriate and adequate measures to protect Private Information in their continued possession and/or control; and (vii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the Private Information compromised as a result

of the Data Breach for the remainder of the lives of Plaintiffs and Illinois Subclass Members.

687. Pursuant to 815 Ill. Comp. Stat. § 505/10a(a), Plaintiffs and the Illinois Subclass seek actual and compensatory damages, injunctive relief, and court costs and attorneys' fees as a result of Defendant's violations of the CFA.

COUNT XVII
Violations of the Washington Consumer Protection Act
Wash. Rev. Code § 19.86.020, *et seq.*
(On Behalf of Plaintiff Cuyle and the Washington Subclass)

688. Plaintiff Cuyle (for the purposes of this count, "Plaintiff") restates and realleges all of the allegations stated above as if fully set forth herein and brings this claim on behalf of herself and the Washington Subclass.

689. Defendant engaged in deceptive, unfair, and unlawful trade acts or practices in the conduct of trade or commerce, in violation of Wash. Rev. Code §19.86.020, including but not limited to omitting, suppressing, and concealing the material fact of the inadequacy of the privacy and security protections for Plaintiff's and Washington Subclass Members' Private Information.

690. Defendant engaged in deceptive, unfair, and unlawful trade acts or practices by failing to maintain the privacy and security of Plaintiff's and Washington 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 Federal Trade Commission Act (15 U.S.C. § 45), HIPAA (42 U.S.C. § 1302d et seq.), and the Washington regulations pertaining to Privacy of Consumer Financial and Health Information (WAC 284-04-300).

691. Defendant engaged in deceptive, unfair, and unlawful trade acts or practices by failing to disclose the Data Breach to Plaintiff and Washington Subclass members in a timely and accurate manner, contrary to the duties imposed by Wash. Rev. Code § 19.255.010(1).

692. Defendant engaged in deceptive, unfair, and unlawful trade acts or practices by failing to take proper action following the Apria Breaches to enact adequate privacy and security measures and protect Plaintiff's and Washington Subclass Members' Private Information from further unauthorized disclosure, release, data breaches, and theft.

693. Defendant's unfair and deceptive acts and practices occurred in trade or commerce insofar as those acts and practices occurred with respect to Defendant's collection and maintenance of Plaintiff's and Washington Subclass Members' Private Information.

694. Defendant's unfair and deceptive acts and practices impacted the public. Defendant collected and maintained Plaintiff's and Washington Subclass Members' Private Information and continues to market its products and services to Plaintiff and Washington Subclass Members.

695. As a direct and proximate result of Defendant's deceptive trade practices, Plaintiff and Washington Subclass members suffered injury and/or damages.

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

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

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

COUNT XVIII
Violations of the Washington Personal Information--Notice Of Security Breaches
Wash. Rev. Code Ann. § 19.255.010(1), *et seq.*
(On Behalf of Plaintiff Cuyle and the Washington Subclass)

699. Plaintiff Cuyle (for the purposes of this count, "Plaintiff") restates and realleges all of the allegations stated above as if fully set forth herein and brings this claim on behalf of herself and the Washington Subclass.

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

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

702. Plaintiff's and Washington Subclass Members' Private Information (e.g., health insurance and medical records, Social Security numbers, and banking and credit card account information) includes personal information as covered under Wash. Rev. Code Ann. § 19.255.005(2)(a) (including e.g., Social Security number, account number or credit or debit card number, full date of birth, health insurance policy number or health insurance identification number, medical history).

703. Because Defendant discovered a breach of its security system (in which personal

information was, or is reasonably believed to have been, acquired by an unauthorized person and the personal information was not secured), Defendant had an obligation to disclose the data breach in a timely and accurate fashion as mandated by Wash. Rev. Code Ann. § 19.255.010(1). However, Defendant breached that obligation. It waited years to notify Plaintiff and the Washington Subclass of its data breach.

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

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

COUNT XIX
Violations of the Washington Uniform Health Care Information Act, Wash. Rev. Code §§ 70.02.020, 70.02.170
(On Behalf of Plaintiff Cuyle and the Washington Subclass)

706. Plaintiff Cuyle (for the purposes of this count, "Plaintiff") restates and realleges all of the allegations stated above as if fully set forth herein and brings this claim on behalf of herself and the Washington Subclass.

707. Defendant is a "health care provider," as defined in Wash. Rev. Code Ann. §§ 70.02.010(15), 70.02.010(19) because it provides health care in the ordinary course of business and is self-described as "a leading provider of home medical equipment and clinical support."[54] Defendant further states "Apria's Care Team members are able to support our patients' treatment plans and supplement with additional services, if needed."[55]

708. As a result of providing healthcare in Washington, Defendant possessed personal

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

information including personal health care information pertaining to Plaintiff and members of the Washington Subclass.

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

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

711. Plaintiff and members of the Washington Subclass seek relief under Wash. Rev. Code § 70.02.170, including but not limited to, actual damages, injunctive relief, and attorneys' fees and costs.

COUNT XX
Violation of the Missouri Merchandising Practices Act,
Mo. Rev. Stat. § 407.010, *et seq.*
(On Behalf of Plaintiff May and the Missouri Subclass)

712. Plaintiffs May and Bennett (for the purposes of this count, "Plaintiffs") restates and realleges all of the allegations stated above as if fully set forth herein and bring this claim on behalf of themselves and the Missouri Subclass.

713. The Missouri Merchandising Practice Act (the "MMPA") prohibits false, fraudulent, or deceptive merchandising practices to protect both consumers and competitors by promoting fair competition in commercial markets for goods and services.

714. The MMPA prohibits the "act, use or employment by any person of any deception, fraud, false pretense, false promise, misrepresentation, unfair practice, or the concealment, suppression, or omission of any material fact in connection with the sale or advertisement of any merchandise in trade or commerce." Mo. Rev. Stat. § 407.020.

715. The MMPA defines "Merchandise" as "any objects, wares, goods, commodities, intangibles, real estate or services." Mo. Rev. Stat. § 407.010(4).

716. Plaintiffs, individually and on behalf of the Missouri Subclass, is entitled to bring an action pursuant to Mo. Rev. Stat. § 407.025, which provides in relevant part that: (a) Any person who purchases or leases merchandise primarily for personal, family or household purposes and thereby suffers an ascertainable loss of money or property, real or personal, as a result of the use or employment by another person of a method, act or practice declared unlawful by section 407.20, may bring a private civil action in either the circuit court of the county in which the seller or lessor resides or in which the transaction complained of took place, to recover actual damages. The court may, in its discretion, award the prevailing party attorneys' fees, based on the amount of time reasonably expended, and may provide such equitable relief as it deems necessary or proper. Mo. Rev. Stat. § 407.025.

717. Defendant is a "person" within the meaning of the MMPA in that Defendant is a domestic, for-profit corporation. Mo. Rev. Stat. § 407.010(5).

718. Plaintiffs and Missouri Subclass Members are "persons" under the MMPA because they are natural persons and they used Defendant's services for personal, family, and/or household use.

719. The Missouri Attorney General has specified the settled meanings of certain terms used in the enforcement of the MMPA. Specifically, Mo. Code Regs. tit. 15, § 60-8.020, provides:

(1) Unfair practice is any practice which—

(A) Either—

1. Offends any public policy as it has been established by the Constitution, statutes, or common law of this state, or by the Federal Trade Commission,

or its interpretive decisions; or

2. Is unethical, oppressive, or unscrupulous; and

(B) Presents a risk of, or causes, substantial injury to consumers.

720. Proof of deception, fraud, or misrepresentation is not required to prove unfair practices as used in section 407.020.1., RSMo. (See Federal Trade Commission v. Sperry and Hutchinson Co., 405 U.S. 233, 92 S.Ct. 898, 31 L.Ed.2d 170 (1972); Marshall v. Miller, 302 N.C. 539, 276 S.E.2d 397 (N.C. 1981); see also, Restatement, Second, Contracts, sections 364 and 365.

721. Pursuant to the MMPA and Mo. Code Regs. Tit. 15, § 60- 8.020, Defendant's acts and omissions fall within the meaning of "unfair."

722. Defendant engaged in a "trade" or "commerce" within the meaning of the MMPA with regard to services which are supposed to keep Plaintiff's and the Missouri Subclass Members's Private Information safe and secure.

723. Defendant engaged in unlawful practices and deceptive conduct in violation of the MMPA by omitting and/or concealing material facts related to the safety and security of Plaintiffs' and the Missouri Subclass Members's Private Information. Defendant's unfair and unethical conduct of failing to secure Private Information and failing to disclose the Data Breach caused substantial injury to consumers in that the type of consumers' personal information impacted by the breach can be used to orchestrate a host of fraudulent activities, including medical, insurance, and financial fraud and identity theft. The impacted consumers have been placed in an immediate and continuing risk of harm from fraud, identity theft, and related harm caused by the Data Breach.

724. Defendant's conduct of failing to secure data required Plaintiffs and the Missouri Subclass to undertake time-consuming, and often costly, efforts to mitigate the actual and potential harm caused by the Data Breach's exposure of their Private Information.

725. Defendant's conduct of concealing, suppressing, or otherwise omitting material facts regarding the Data Breach was likely to mislead reasonable consumers under the circumstances, and thus constitutes an unfair and deceptive trade practice in violation of the MMPA.

726. By failing to secure sensitive data and failing to disclose and inform Plaintiffs and Missouri Subclass Members about the Breach of Private Information, Defendant engaged in acts and practices that constitute unlawful practices in violation of the MMPA. Mo. Ann. Stat. §§ 407.010, et seq.

727. Defendant engaged in unlawful practices and deceptive conduct in the course of their business that violated the MMPA including misrepresentations and omissions related to the safety and security of Plaintiff's and the Missouri Subclass's Private Information. Mo. Rev. Stat. § 407.020.1.

728. As a direct and proximate result of these unfair and deceptive practices, Plaintiffs and each Missouri Subclass member suffered actual harm in the form of money and/or property because the disclosure of their Private Information has value encompassing financial data and tangible money.

729. Defendant's unlawful conduct also included omitting material facts, such as the following failures:

a. Implementing inadequate data security systems, practices, and protocols to prevent data loss;

b. Failure to mitigate the risks of a possible data breach and Plaintiff's and the Missouri Subclass's loss of data;

c. Failure to ensure the confidentiality, integrity, and availability of all electronic

protected health information;

d. Failure to ensure Plaintiffs' and the Missouri Subclass's confidentiality and integrity of electronic Private Information;

e. Failure to implement policies and procedures that successfully prevent, detect, contain, and correct security violations;

f. Failure to mitigate, to the extent practicable, harmful effects of security incidents that were known or should have been known;

g. Failure to protect against reasonably anticipated threats or hazards to the security or integrity of Private Information;

h. Failure to protect against any reasonably anticipated disclosures of Private Information that were not permitted under the privacy rules regarding individually identifiable health information.

730. Defendant's misrepresentations and omissions were material to consumers and made in order to induce consumers' reliance regarding the safety and security of Private Information in order to obtain consumers' Private Information and purchase of healthcare services.

731. Defendant's deceptive practices misled Plaintiffs and the Missouri Subclass and would cause a reasonable person to enter into transactions with Defendant that resulted in damages.

732. As such, Plaintiffs and the Missouri Subclass seek: (1) to recover actual damages sustained; (2) to recover punitive damages; (3) to recover reasonable attorneys' fees and costs; and (4) such equity relief as the Court deems necessary or proper to protect Plaintiff and the members of the Missouri Subclass from Defendant's deceptive conduct and any other statutorily available damages or relief the court deems proper.

COUNT XXI
Violation Of The New York Deceptive Trade Practices Act ("GBL")

New York Gen. Bus. Law § 349
(On Behalf of Plaintiff Munoz and the New York Subclass)

733. Plaintiff Munoz (for the purposes of this count, "Plaintiff") restates and realleges all of the allegations stated above as if fully set forth herein and bring this claim on behalf of themselves and the New York Subclass.

734. Defendant engaged in deceptive, unfair, and unlawful trade acts or practices in the conduct of trade or commerce and furnishing of services, in violation of N.Y. Gen. Bus. Law § 349(a), including, but not limited to, the following:

a. Misrepresenting material facts to Plaintiff and the New York Subclass by representing that they would maintain adequate data privacy and security practices and procedures to safeguard New York Subclass Members' Private Information from unauthorized disclosure, release, data breaches, and theft;

b. Misrepresenting material facts to Plaintiff and the New York Subclass by representing that they did and would comply with the requirements of federal and state laws pertaining to the privacy and security of New York Subclass Members' Private Information;

c. Omitting, suppressing, and/or concealing material facts of the inadequacy of its privacy and security protections for New York Subclass Members' Private Information;

d. Engaging in deceptive, unfair, and unlawful trade acts or practices by failing to maintain the privacy and security of New York Subclass Members' Private Information, in violation of duties imposed by and public policies reflected in applicable federal and state laws; and,

e. Engaging in deceptive, unfair, and unlawful trade acts or practices by failing to

disclose the Data Breach to the New York Subclass in a timely and accurate manner, contrary to the duties imposed by N.Y. Gen. Bus. Law § 899-aa(2).

735. Defendant knew or should have known that its network and data security practices were inadequate to safeguard the New York Subclass Members' Private Information entrusted to it, and that risk of a data breach or theft was highly likely.

736. Defendant should have disclosed this information because Defendant was in a superior position to know the true facts related to the defective data security.

737. Defendant's failure constitutes false and misleading representations, which have the capacity, tendency, and effect of deceiving or misleading consumers (including Plaintiff and New York Subclass Members) regarding the security of Defendant's network and aggregation of Private Information.

738. The representations upon which current and former patients (including Plaintiff and New York Subclass Members) relied were material representations (e.g., as to Defendant's adequate protection of Private Information), and Plaintiff a New York Subclass Members relied on those representations to their detriment.

739. Defendant's conduct is unconscionable, deceptive, and unfair, as it is likely to, and did, mislead consumers acting reasonably under the circumstances. As a direct and proximate result of Defendant's conduct, Plaintiff and other New York Subclass Members have been harmed, in that they were not timely notified of the Data Breach, which resulted in profound vulnerability to their personal information and other financial accounts.

740. Defendant knew or should have known that their computer systems and data security practices were inadequate to safeguard New York Subclass Members' Private Information and that the risk of a data security incident was high.

741. Defendant's acts, practices, and omissions were done in the course of Defendant's business of furnishing healthcare services to consumers in the State of New York.

742. As a direct and proximate result of Defendant's unconscionable, unfair, and deceptive acts and omissions, Plaintiff's and New York Subclass Members' Private Information was disclosed to third parties without authorization, causing and will continue to cause Plaintiff and New York Subclass Members damages.

743. Plaintiff and New York Subclass Members were injured because:

a) Plaintiff and New York Subclass Members would not have paid Defendant for services had they known the true nature and character of Defendant's data security practices;

b) Plaintiff and New York Subclass Members would not have entrusted their Private Information to Defendant in the absence of promises that Defendant would keep their information reasonably secure, and

c) Plaintiff and New York Subclass Members would not have entrusted their Private Information to Defendant in the absence of the promise to monitor their computer systems and networks to ensure that they adopted reasonable data security measures.

744. As a direct and proximate result of Defendant's multiple, separate violations of GBL §349, Plaintiff and the New York Subclass Members suffered damages including, but not limited to: (i) invasion of privacy; (ii) loss of benefit of the bargain; (iii) lost time, spent on activities remedying harms resulting from the Data Breach; (iv) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; and (v) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available

for unauthorized third parties to access and abuse; and (b) remain backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information.

745. As a result, Plaintiff and the New York Subclass Members have been damaged in an amount to be proven at trial.

746. Plaintiff brings this action on behalf of herself and New York Subclass Members for the relief requested above and for the public benefit to promote the public interests in the provision of truthful, fair information to allow consumers to make informed purchasing decisions and to protect Plaintiff, New York Subclass Members and the public from Defendant's unfair, deceptive, and unlawful practices. Defendant's wrongful conduct as alleged in this Complaint has had widespread impact on the public at large.

747. Plaintiff and New York Subclass Members seek relief under N.Y. Gen. Bus. Law § 349(h), including, but not limited to, actual damages, treble damages, statutory damages, injunctive relief, and/or attorneys' fees and costs.

748. On behalf of herself and other members of the New York Subclass, Plaintiff seeks to enjoin the unlawful acts and practices described herein, to recover her actual damages or fifty dollars, whichever is greater, three times actual damages, and reasonable attorneys' fees.

COUNT XXII
Declaratory Judgment
(On Behalf of Plaintiffs and the Class)

749. Plaintiffs restate and reallege all of the allegations stated above as if fully set forth herein.

750. 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.

751. An actual controversy has arisen in the wake of the Apria data breach regarding its present and prospective common law and other duties to reasonably safeguard consumers' personally identifiable information in its possession, custody, and/or control and regarding whether Apria is currently maintaining data security measures adequate to protect Plaintiffs and class members from further data breaches that compromise their personal information. Plaintiffs continue to suffer injury as a result of the compromise of their personal information and remain at imminent risk that further compromises of their personal information will occur in the future.

752. Apria owes duties of care to Plaintiffs and the Class Members that require it to adequately secure Plaintiffs' and Class Members' Private Information.

753. Apria still possesses Private Information regarding Plaintiffs and Class Members.

754. Plaintiffs allege that Apria's data security measures remain inadequate. Apria publicly denies these allegations. Furthermore, Plaintiffs 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.

755. 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.

756. The Court should issue corresponding prospective injunctive relief requiring Apria to employ adequate security protocols consistent with law and industry standards to protect Plaintiffs' and class members' personal information, including:

a. Requiring Apria 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:

b. 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;

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

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

e. 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;

f. Conducting regular database scanning and securing checks;

g. Implementing two-factor authentication

h. 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;

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

j. 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 themselves.

757. 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.

758. If an injunction is not issued, Plaintiffs and 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, Plaintiffs will not have an adequate remedy at law because many of the resulting injuries are not readily quantifiable.

759. The hardship to Plaintiffs and Class Members if an injunction does not issue exceeds the hardship to Apria if an injunction is issued. Plaintiffs 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.

760. 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 Plaintiffs and Class Members whose Private Information would be further compromised.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and all others similarly situated, respectfully request judgment against Apria and that the Court grants the following:

A. For an Order certifying this action as a class action and appointing Plaintiffs and their counsel to represent the Class, California Subclass, Illinois Subclass, New York Subclass, Missouri Subclass, and Washington Subclass, pursuant to Federal Rule of Civil Procedure 23;

B. For equitable relief enjoining Apria from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiffs' and class members' Private Information, and from refusing to issue prompt, complete and accurate disclosures of the Data Breach to Plaintiffs and class members;

C. For injunctive relief requested by Plaintiffs, including, but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiffs and class members, including but not limited to an order:

i. prohibiting Apria from engaging in the wrongful and unlawful acts described herein;

ii. requiring Apria to protect, including through encryption, all data collected through the course of their business in accordance with all applicable regulations, industry standards, and federal, state or local laws;

iii. requiring Apria delete, destroy, and purge the personal identifying information of Plaintiffs and class members unless Apria can provide to the

Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiffs and class members;

iv. requiring Apria to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the Private Information of Plaintiffs and class members;

v. prohibiting Apria from maintaining the Private Information of Plaintiffs and class members on a cloud-based database;

vi. requiring Apria to engage independent 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;

vii. requiring Apria to engage independent third-party security auditors and internal personnel to run automated security monitoring;

viii. requiring Apria to audit, test, and train their security personnel regarding any new or modified procedures; requiring Apria to segment data by, among other things, creating firewalls and access controls so that if one area of Apria's network is compromised, hackers cannot gain access to other portions of Apria's systems;

ix. requiring Apria to conduct regular database scanning and securing checks;

x. requiring Apria to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees'

respective responsibilities with handling personal identifying information, as well as protecting the personal identifying information of Plaintiffs and Class Members;

xi. requiring Apria to routinely and continually conduct internal training and education, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

xii. requiring Apria to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees compliance with Apria's policies, programs, and systems for protecting personal identifying information;

xiii. requiring Apria to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Apria's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

xiv. requiring Apria to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves;

xv. requiring Apria to implement logging and monitoring programs sufficient to track traffic to and from Apria's servers; and

xvi. for a period of 10 years, appointing a qualified and independent third-party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Apria's compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court's final judgment;

D. For an award of actual damages, compensatory damages, statutory damages, and nominal damages, in an amount to be determined, as allowable by law;

E. For an award of punitive damages, as allowable by law;

F. For an award of attorneys' fees and costs, and any other expenses, including expert witness fees;

G. Pre- and post-judgment interest on any amounts awarded; and

H. Such other and further relief as this court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiffs demand a trial by jury on all triable issues.

DATED: October 23, 2023

Respectfully submitted,

/s/ Kathleen A. DeLaney

Kathleen A. DeLaney (#18604-49)
DELANEY & DELANEY LLC
3646 North Washington Blvd.
Indianapolis, IN 46205
Telephone: (317) 920-0400
Email: kathleen@delaneylaw.net

Plaintiffs' Interim Liaison Counsel

Lynn A. Toops (No. 26386-49)
Mary Kate Dugan (No. 37623-49)
Natalie A. Lyons (No. 36583-63)
COHEN & MALAD, LLP
One Indiana Square, Suite 1400

Indianapolis, Indiana 46204
(317) 636-6481
ltoops@cohenandmalad.com
mdugan@cohenandmalad.com
nlyons@cohenandmalad.com

Gary M. Klinger
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
227 W. Monroe Street, Suite 2100
Chicago, IL 60606
Phone: 866-252-0878
gklinger@milberg.com

Plaintiffs' Interim Co-Lead Counsel

Mason A. Barney
Tyler J. Bean (pro hac vice)
SIRI & GLIMSTAD LLP
745 Fifth Avenue, Suite 500
New York, New York 10151
Telephone: (212) 532-1091
Email: mbarney@sirillp.com
Email: tbean@sirillp.com

M. Anderson Berry
Gregory Haroutunian
Brandon P. Jack (pro hac vice forthcoming)
CLAYEO C. ARNOLD, A PROFESSIONAL CORPORATION
865 Howe Avenue
Sacramento, CA 95825
Telephone: (916) 239-4778
Facsimile: (916) 924-1829
Email: aberry@justice4you.com
Email: gharoutunian@justice4you.com
Email: bjack@justice4you.com

Kim D. Stephens, P.S. (pro hac vice forthcoming)
Kaleigh N. Boyd
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

Stephen R. Basser (pro hac vice forthcoming)
Samuel M. Ward (pro hac vice forthcoming)
BARRACK, RODOS & BACINE
600 West Broadway, Suite 900
San Diego, CA 92101
Telephone: (619) 230-0800
Facsimile: (619) 230-1874
sbasser@barrack.com

Plaintiffs' Executive Committee

Counsel for Plaintiffs and the Proposed Class