EXHIBIT A(13)

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

ILYA RABINOVICH,	)	
	)	
Plaintiff,	)	
	)	
vs.	)	CAUSE NO. 1:23-cv-1205
	)	
APRIA HEALTHCARE, LLC,	)	
	)	
Defendant.	)	
	)	

CLASS ACTION COMPLAINT

Plaintiff Ilya Rabinovich ("Plaintiff"), individually and on behalf of all others similarly situated (putative "Class Members"), brings this data breach Class Action Complaint against Defendant Apria Healthcare LLC ("Defendant" or "Apria") and alleges, upon personal knowledge as to his own actions and the investigation of counsel, and upon information and belief as to all other matters, as follows:

NATURE OF THE ACTION

1. Apria touts itself as a "leading provider of home healthcare equipment and related services across the USA, serving approximately 2 million patients from our 280 locations."[1] Apria states that "[p]atient satisfaction is at the heart of everything we do at Apria. The lives of those we serve are directly impacted by the care we provide, and it is our commitment to provide top quality service that exceeds our patients' expectations." *Id.*

2. In the ordinary course of business Defendant collects, maintains, and stores its customers' highly sensitive personally identifying information ("PII"), including Social Security numbers, dates of birth, full names, addresses, drivers' license numbers, health insurance

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

information and telephone numbers, along with customer protected health information ("PHI"), including medical and laboratory testing, diagnosis and treatment information, as well as customer health insurance information.

3. Apria states that it's "[e]xtensive Medicare experience as well as the largest network of payor contracts, helps ensure that Apria is positioned to provide care to more patients than any other healthcare provider. We take our role as a leading provider of home healthcare services seriously, acting as an industry-leading innovator.[2] In its Privacy Policy, Apria states that it "respects the privacy of your information."

4. Regarding PII, Apria states on its website: "[t]o ensure that your Personally Identifiable Information receives an adequate level of protection, we have put in place appropriate procedures with the service providers we share it with to ensure that it is treated consistent with applicable data security and privacy laws...."[3] Regarding PHI, Apria states on its website: "[we] are required by law to maintain the privacy of your protected health information ("PHI"), to provide you with this Notice of our legal duties and privacy practices with respect to your PHI, and to notify you if a breach of your PHI occurs, in accordance with applicable law. When we use or disclose your PHI, we are required to abide by the terms of this Notice (or other notice in effect at the time of the use or disclosure)."[4]

5. Apria's assurances of "adequate [] protection" is plainly false -- as a direct and proximate result of Defendant's failure to implement reasonable security protections sufficient to prevent a foreseeable and avoidable ransomware cyberattack, as relayed by Defendant, between April 5, 2019 and May 7, 2019 and again between August 27, 2021 and October 10, 2021,

[2] *Id.*
[3] https://www.apria.com/privacy-policy
[4] https://www.apria.com/hipaa-privacy-notice; https://www.apria.com/hubfs/GEN-4539_Form_Notice-Privacy-Practices_04-22_v2_FNL.pdf

unauthorized actors compromised Defendant's network, accessed, and extracted highly-sensitive PII and PHI information of more than 1.8 million of Apria's customer patients, including the Plaintiff and putative Class Members ("the Data Breach").

6. Although Defendant's systems were breached in both 2019 and 2021, Defendant did not timely notify Plaintiff and Class Members of the Data Breach and/or inform them that their PII and PHI was compromised until May 22, 2023 (the "Notice Letter"), **years** after the Data Breach occurred.

7. The Notice Letter informed its members that:

> "On September 1, 2021, Apria []received a notification regarding access to select Apria systems by an unauthorized third party. Apria took immediate action to mitigate the incident, including working with the Federal Bureau of Investigation (FBI) and hiring a reputable forensic investigation team to investigate and securely resolve the incident. An unauthorized third party accessed systems which contained personal information from April 5, 2019 to May 7, 2019 and from August 27, 2021 to October 10, 2021.

8. The requirements of prompt notification to impacted individuals under the Health Insurance Portability and Accountability Act ("HIPAA"), discussed in detail below at 27-41, were plainly neglected, raising "serious questions about the company's cybersecurity practices" given the duration and number of times the unauthorized actors accessed Apria's systems.[5]

9. Accordingly, Plaintiff and Class Members were not aware that their PII and PHI had been compromised, and that they were, and continue to be, at significant risk of identity theft and various other forms of personal, social, and financial harm.

10. As a result, there is an increased and substantial risk that Plaintiff and Class Members will experience an increased risk to the compromise of their PII and PHI.

[5] https://www.cpomagazine.com/cyber-security/apria-healthcare-data-breach-exposed-sensitive-information-of-nearly-2-million-patients/

11. Defendant disregarded Plaintiff's and Class Members' rights by, among other things, intentionally, willfully, recklessly, and/or negligently failing to take and implement adequate and reasonable measures to ensure that Plaintiff's and Class Members' PII and PHI stored within Defendant's information system were protected and safeguarded against unauthorized access, misuse, and disclosure, failing to take basic industry-standard steps to prevent, identify, contain a breach of its system's security, failing to follow applicable, required and appropriate protocols, policies and procedures regarding the encryption of data, even for internal use, and failing to give timely and adequate notice to Plaintiff and Class Members that their PII and PHI had been subject to the unauthorized access of an unknown third party.

12. Plaintiff and Class Members suffered injuries as a result of Defendant's conduct including, but not limited to: lost or diminished value of their PII; out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to the loss of time needed to take appropriate measures to avoid unauthorized and fraudulent charges; time needed to change usernames and passwords on their accounts; time needed to investigate, correct and resolve unauthorized access to their accounts; time needed to deal with spam messages and e-mails received subsequent to the Data Breach; charges and fees associated with fraudulent charges on their accounts; and the continued and increased risk of compromise to their PII, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect their PII. These risks will remain for the lifetimes of Plaintiff and the Class Members.

13. Accordingly, Plaintiff brings this Class Action Complaint on behalf of all those similarly situated persons – the Class Members -- whose PII and PHI was compromised as a result

of Defendant's negligence, violations of federal and state statutes, and on other grounds, in failing to: (i) adequately protect their PII and PHI; (ii) adequately warn them of Defendant's inadequate information security practices; (iii) adequately secure computer systems and hardware containing protected PII and PHI using reasonable and effective security measures free of vulnerabilities and incidents; and (iv) failure to timely warn them of the Data Breach.

14. Plaintiff and the Class Members seek all available remedies, including but not limited to statutory and nominal damages, compensatory damages for identity theft, fraud, and time spent, reimbursement of out-of-pocket costs, adequate credit monitoring services funded by Defendant, and injunctive relief including improvements to Defendant's data security systems and practices to ensure they have reasonably sufficient security practices to safeguard their customers' PII and PHI that remains in Defendant's custody to prevent incidents like the Data Breach from reoccurring in the future.

PARTIES

15. Plaintiff Ilya Rabinovich is and has been, at all relevant times, a resident and citizen of the State of Colorado. Plaintiff received a copy of the May 23, 2023, Notice Letter, via U.S. mail, from Apria on or about June 25, 2023.

16. Plaintiff Rabinovich provided his PII and PHI to Defendant in connection with home healthcare equipment he received from Apria and provided that information on the condition that it be maintained as confidential and with the understanding that Defendant would employ reasonable safeguards to protect that information. If Mr. Rabinovich had known that Defendant would not adequately protect his PHI and PII, he would not have entrusted Defendant with that information and would have sought the services, including insurance, of other providers.

17. Defendant Apria is a leading provider of home healthcare equipment, serving over 2 million patients from over 200 locations in the United States, with its principal place of business located at 7353 Company Drive, Indianapolis, Indiana, 46237.

JURISDICTION AND VENUE

18. This Court has subject matter jurisdiction pursuant to the Class Action Fairness Act of 2005 ("CAFA"), 28 U.S.C. § 1332(d). The amount in controversy exceeds the sum of $5,000,000 exclusive of interest and costs, there are more than 100 putative class members, and minimal diversity exists because many putative class members are citizens of a different state than Defendant. This Court also has supplemental jurisdiction pursuant to 28 U.S.C. § 1367(a) because all claims alleged herein form part of the same case or controversy.

19. This Court has personal jurisdiction over Defendant because Defendant operates and maintains its principal place of business in this District and the computer systems implicated in this Data Breach are likely based in this District. Further, Defendant is authorized to and regularly conducts business in this District and makes decisions regarding corporate governance and management of its businesses in this District, including decisions regarding the security measures to protect its customer patients' PII and PHI.

20. Venue is proper in this District under 28 U.S.C. § 1391(a) through (d) because a substantial part of the events giving rise to this action occurred in this District, including decisions made by Defendant's governance and management personnel or inaction by those individuals that led to the Data Breach; Defendant is headquartered in this District; Defendant maintains Plaintiff's and Class Members' PII and PHI in this District; and Defendant caused harm to Plaintiff and Class Members from within this District.

STATEMENT OF FACTS

Background

21. Apria is one of the nation's leading providers of home respiratory services and medical equipment including oxygen therapy, inhalation therapies, sleep apnea treatment, and negative pressure wound therapy.

22. Plaintiff and Class Members are current and former Apria customer patients who obtained services and/or equipment from Defendant.

23. To obtain services and/ or equipment from Defendant, Plaintiff and Class Members were required to provide – and Apria was required to collect and maintain -- sensitive and confidential PII and PHI, including customer patient names, Social Security numbers, health insurance information, and sensitive health care information, which Apria stored and maintained in its computer systems. Indeed, by their nature Apria's customer patient health testing, treating and insuring -- the PHI at issue is incredibly sensitive information.

24. Defendant relies extensively on technology systems and networks to provide many of its services including the ordering of supplies and bill payment, along with its customer patients' PII and PHI which are critical to Defendant's core business operations.

25. Defendant uses the PII and PHI it collects to create and maintain records stored in digital format on hardware, such as computers, mobile devices, flash drives, off-site "clouds" or similar storage devices and means, and that are transmitted, shared, or accessed through Apria's networks.

26. By obtaining, collecting, storing, using, disseminating the PII and PHI it collects from Plaintiff and Class Members, Defendant derives substantial economic benefits. For example, Defendant gathers, creates, and distributes customer plaintiff health information as its customer patients authorize to doctors, nurses, clinicians, technicians, staff, and other healthcare

professionals who become involved in a customer patient's health care to provide, coordinate, or manage that patient's healthcare, including providing healthcare equipment, products, supplies and therapies. Such data is a core part of Apria's business operations. Apria receives payment for the healthcare services it has provided and the related information (PII and PHI) obtained from or for the benefit of Apria's customer patients' other health care providers for diagnosis and treatment.

HIPAA Requirements To Protect PII and PHI Data

27. Defendant is a covered entity under HIPAA (45 C.F.R. § 160.102) and is required to comply with the HIPAA Privacy Rule and Security Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and E ("Standards for Privacy of Individually Identifiable Health Information"), and Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C. Thus, HIPAA requires Defendant's "compl[iance] with the applicable standards, implementation specifications, and requirements" of HIPAA "with respect to electronic protected health information." 45 C.F.R. § 164.302. "Electronic protected health information" is "individually identifiable health information … that is (i) transmitted by electronic media; maintained in electronic media." 45 C.F.R. § 160.103.

28. Defendant is also subject to the rules and regulations for safeguarding electronic forms of medical information pursuant to the Health Information Technology Act ("HITECH"). *See* 42 U.S.C. §17921, 45 C.F.R. § 160.103.

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

30. HIPAA and HITECH 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.

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

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

33. HIPAA's Security Rule requires Defendant to:

a. Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits;
b. Protect against any reasonably anticipated threats or hazards to the security or integrity of such information; Protect against any reasonably anticipated uses or disclosures of such information that are not permitted; and
c. Ensure compliance by its workforce.

34. HIPAA requires Defendant to "review and modify the security measures implemented … as needed to continue provision of reasonable and appropriate protection of electronic protected health information." 45 C.F.R. § 164.306(e).

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

36. The HIPAA Breach Notification Rule, 45 C.F.R. §§ 164.400-414, requires Defendant to provide notice of the Data Breach to each affected individual "without unreasonable delay and ***in no case later than 60 days following discovery of the breach***."

37. 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).

38. 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).

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

40. In sum, HIPAA requires, among other things, that Defendant implement and maintain policies, procedures, systems and safeguards that ensure the confidentiality and integrity of consumer and patient PII and PHI, protect against any reasonably anticipated threats or hazards to the security or integrity of consumer and patient PII and PHI, regularly review access to data bases containing protected information, and procedures and systems to detect, contain, and correct

any unauthorized access to protected information. *See* 45 CFR § 164.302, et seq. Additionally, HIPAA requires that Defendant provide adequate and timely notification to every affected individual following the impermissible use or disclosures of any PHI. Individual notice must be provided to affected individuals without unreasonable delay. Further, for a breach involving more than 500 individuals such the Data Breach involving Defendant, entities are required to provide notice in prominent media outlets. *See* 45 CFR § 164.400, et seq.

41. In the ordinary course of its business as required by law, Defendant must provide every customer patient with a HIPAA compliant disclosure form in which it represents that it will protect patient customer PII and PHI, including that of Plaintiff and Class Members.

FTC Requirements To Protect PII and PHI Data

42. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices to prevent data breaches. According to the FTC, the need for data security should be factored into all business decision- making.

43. 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 businesses, such as Defendant, of failing to use reasonable measures to protect Private Information.

44. The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number,

alien registration number, government passport number, employer or taxpayer identification number." *Id.*

45. The FTC has issued numerous guides for businesses highlighting the importance of reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-marking.

46. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established guidelines for fundamental data security principles and practices for business. The guidelines note businesses should protect the personal information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct security problems.

47. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.

48. The FTC recommends that companies not maintain PII and PHI longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

49. The FTC's Health Breach Notification Rule obligates companies that suffered a data breach to provide notice to every individual affected by the data breach, as well as notifying the media and the FTC. *See* 16 CFR 318.1, et seq.

50. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations. These FTC enforcement actions include actions against healthcare entities, like Defendant. *See, e.g., In the Matter of LabMD, Inc., a corp*, 2016-2 Trade Cas. (CCH) ¶ 79708, 2016 WL 4128215, at *32 (MSNET July 28, 2016) ("[T]he Commission concludes that LabMD's data security practices were unreasonable and constitute an unfair act or practice in violation of Section 5 of the FTC Act.").

SOC 2 Type 2 Attestation Requirements

51. One of the services provided by auditors is to evaluate and report on a company's System and Organization Control ("SOC"). SOC reporting attests to whether the company has adequate controls relevant to its data security, data processing integrity of the systems it uses to process data, and the confidentiality and privacy of the information processed by these systems.

52. SOC 2 audits utilize AICPA's Trust Services Criteria (TSC) framework and its Trust Services Principles (TSP):

- **Security** – Prevention of unauthorized or harmful uses and disclosures of data;
- **Availability** – Accessibility of user-facing systems and information at all times;
- **Process Integrity** – Completeness, timeliness, and authorization of all processes;
- **Confidentiality** – Protection against breaches of legally protected information; and
- **Privacy** – Protection against breaches of personally identifiable information.

53. A SOC 2 attestation is a report on an organization's ability to ensure some combination of these principles to its clients. It may focus on all five or a selection thereof and is generated for a specialized audience.

54. To prevent and detect cyber-attacks Defendant could and should have sought a SOC 2 audit, which would have ensured the security and availability of its information management systems and data. Such an attestation would have built trust in its operations across current and future clients.

Cyber Security Industry Standards To Protect PII and PHI Data

55. Cyber security industry experts routinely identify entities, like Defendant, that collect, store and utilize PII and PHI as being particularly vulnerable to cyberattacks because of the tremendous value of that information to cyber criminals.

56. Several best practices have been identified that, at a minimum, should be implemented by healthcare entities in possession of PII and/or PHI, like Defendant, including but not limited to:

- educating all employees;
- strong passwords;
- multi-layer security, including firewalls, anti-virus, and anti-malware software;
- encryption, making data unreadable without a key;
- multi-factor authentication; and
- backup data and limiting which employees can access sensitive data.

57. Other standard best cybersecurity industry practices that are applicable in the healthcare industry to entities such as Defendant that collect, store and utilize customer patient PII and/or PHI 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, as identified in part by the following cybersecurity frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1,

DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

Defendant's Knowledge of HIPAA, FTC and Industry Standards & Representations To Plaintiff and Class Members to Protect their PII and PHI Data

58. Defendant holds itself out as respecting customer patients' privacy to gain the trust of its customer patients who use its products and services, including Plaintiff and Class Members.

59. Defendant knows, and is required to know, of HIPAA, FTC, and cyber security industry standards, guidelines and legal requirements to protect the PII and PHI of its customer patients, including Plaintiff and Class Members, from such cyberattacks and data breaches.

60. Such knowledge is reflected in the fact that Defendant represents to its customer patients, including Plaintiff and Class Members, that they will comply with PII and PHI data privacy and security requirements, including those implemented by HIPAA, the FTC, and industry standards regarding the protection of PII and PHI and prompt and adequate notification of data breaches.

61. Defendant directly and implicitly represented to its customer patients, including Plaintiff and Class Members, that the PII and PHI they provided to Apria and/or that Apria collected on their behalf for their benefit, including as a condition of submitting an application and other documentation for Apria's health care and services and products, would be kept safe, confidential, and private and that Apria would not permit the disclosure of such information to anyone other than whom Plaintiff and Class Members explicitly authorized.

62. Defendant made express and implied representations concerning its commitment to user privacy, data security, and regulatory compliance that would lead a reasonable person in similar circumstances to believe that Defendant had, has, and will maintain in place reasonable

cybersecurity practices and procedures to protect from unlawful use or disclosure of any customer patient's PII and PHI they collect or maintain in the regular course of business. Indeed, Apria's Privacy Policy provides:

Introduction
Apria Healthcare LLC and its affiliates ("Apria," "we," "our," or "us") respects the privacy of your information. This Privacy Policy is designed to assist you in understanding how we collect, use and safeguard the information you provide to us in using Apria.com, My.Apria.com, and the websites that link to this Privacy Policy (collectively, the "Site") and the services provided through our Site (collectively, the "Services").

We will use and share any personal health information governed by HIPAA and HITECH (each defined herein) that we collect from or about you in accordance with our HIPAA Notice of Privacy Practices, which offers you certain choices with respect to the use and sharing of that personal information.

1. Personal Data We Collect
We collect personal data from you through your use of the Site and Services. Personal data is information that is linked or reasonably linkable to an identified or identifiable individual. We collect the following types of personal data:

Personal Data You Provide

We may collect the following personal data that you voluntarily provide to us in using our Site and Services:

- *Customer Account.* If you create an account for any of our Services, you will provide us with your phone number, email address, and password. When you log-in to your account, you will provide us with your email address and password.
- *Check a Delivery Time.* When you use our Site to obtain your estimated time of delivery, you will provide us with the patient's name, date of birth, customer ID, and delivery address.
- *Continuous Sleep Resupply Program*. When you enroll in this program on our Site, you will provide us with your name, email address, physical address, and any other information that you may voluntarily provide.
- *Preventative Maintenance Check for Your Oxygen Concentrator.* When you schedule a Preventative Maintenance Check for Your Oxygen Concentrator on our Site, you will provide us with your name, email address, physical address, and phone number along with the patient's name, ID, and any other information that you may voluntarily provide.
- *Schedule an Oxygen Tank Delivery*. When you schedule an Oxygen Tank Delivery on our Site, you will provide us with your name, email address, physical address, and phone number along with the patient's name, ID, and any other information that you may voluntarily provide.

- *Schedule an Equipment Return*. When you schedule an Equipment Return on our Site, you will provide us with your name, email address, physical address, and phone number along with the patient's name, ID, and any other information that you may voluntarily provide.
- *ApriaLink Registration*. If you are a healthcare provider or an employee of a healthcare provider and you submit a Physician/Prescriber Registration Form, you will provide us with your name, email address, company name, physical address, and National Provider Identifier (NPI) number. When you submit a Non-Physician/Prescriber Registration Form, you will provide us with your name, email address, company name, and physical address.
- *Careers*. When you apply for a job, you will create a profile and provide us with your name, email address, telephone number, physical address, and other identifiers such as licenses and certifications and any other information that you may voluntarily provide.
- *Billing Inquiry*. When you submit a question about billing on our Site, you will provide us with your name, email address, phone number, patient account number, and any other information that you may voluntarily provide.
- *Dispute Resolution.* When you submit an Opt-out Arbitration Form on our Site, you will provide us with your name and email address along with the patient's name, ID, physical address, and any other information that you may voluntarily provide.
- *Patient Satisfaction*. When you submit a Patient Satisfaction form on our Site, you may provide us with name, email address, physical address, phone number, patient name, and any other information that you may voluntarily provide.
- *Apria Pharmacy*. When you submit an inquiry to Apria Pharmacy on our Site, you will provide us with your relationship to the patient, email address, physical address, phone number, the patient's name and ID, and any other information that you may voluntarily provide.
- *Chat with Us*. When you interact with our Live Chat on Apria.com, you may provide us with information, such as your name, email address, and phone number, as well as any information you choose to provide in your message. Our chat feature is provided by Zendesk. Zendesk may collect, record, and store the information you provide in the chat. Please review Zendesk's privacy notice here.
- *Additional Information*. When you submit information on the Site, send an email from the Site, place an order, enter a contest or sweepstakes, respond to a survey or communication, submit an inquiry such as email, or participate in another Site function or feature, you may provide us with other information.

You may use your account to access, correct, or view certain personal data we have collected and which is associated with your account. To review or request changes to any of your personal data, please contact us at SG-privacy@apria.com.

Personal Data as You Navigate Our Site

We automatically collect certain personal data through your use of the Site and our use of cookies and other tracking technologies, such as the following:

- *Usage Information*. For example, the pages on the Site you access, the frequency of access, and what you click on while on the Site.

- *Device Information*. For example, hardware model, operating system, application version number, and browser.
- *Mobile Device Information*. Aggregated information about whether the Site is accessed via a mobile device or tablet, the device type, and the carrier.
- *Location Information*. Location information from Site visitors on a city-regional basis.

For more information on our cookie usage see our "Cookies and Other Tracking Technologies" section below.

Personal Data We Collect About You from Other Sources

In some cases, we may receive personal data about you from other sources. This may include government entities, advertising networks, operating systems and platforms, and marketing partners.

2. How We Use Your Personal Data

We use the personal data we collect to provide the Services to you, to maintain and improve our Site and Services, and to protect our legal rights and the rights of others. In addition, we may use the personal data we collect to:

- Personalize your Site experience and to allow us to deliver the type of content and product offerings in which you may be most interested;
- Process your transactions and communicate with you regarding your order;
- Confirm your order;
- Deliver the products and Services that you purchase or rent on our Site;
- Prevent fraud and bill you for your purchases;
- Contact you regarding our products and services that we feel may be of interest to you;
- Administer a contest, promotion, survey, or other Site feature;
- Communicate with you about our Site or Services or to inform you of any changes to our Site or Services;
- Provide support; and
- Comply with applicable law.[6]

63. In discussing the private and confidential nature of a patient's medical information and Apria's requirement to maintain the privacy of protected health information, the following is provided:

How We May Share Your Personal Data

We may share the personal data that we collect about you in the following ways:

- With vendors who perform data or Site-related services on our behalf (e.g., email, hosting, maintenance, backup, analysis, etc.);

[6] https://www.apria.com/privacy-policy

- To the extent that we are required to do so by law;
- In connection with any legal proceedings or prospective legal proceedings;
- To establish, exercise, or defend our or a third party's legal rights, including providing information to others for the purposes of fraud prevention;
- With any person who we reasonably believe may apply to a court or other competent authority for disclosure of that personal data where, in our reasonable opinion, such court or authority would be reasonably likely to order disclosure of that personal data;
- With any other person or entity as part of any business or asset sale, equity transaction, merger, acquisition, bankruptcy, liquidation, or similar proceeding, or in preparation for any of these events;
- With any other person or entity where you consent to the disclosure; and
- For any other purpose disclosed by us when you provide the personal data or for any other purpose we deem necessary, including to protect the health or safety of others.

Where appropriate, we will limit sharing of your information in accordance with the choices you have provided us in response to our HIPAA Notice of Privacy Practices.[7]

Plaintiff And Class Members' Provision of PII and PHI To Defendant

64. Plaintiff and Class Members value the privacy and confidentiality of their Private Information and take reasonable steps to protect and maintain the confidentiality of their own PII and PHI.

65. Plaintiff and Class Members were required to provide to Defendant, and/or permit Defendant to acquire, their PII and PHI in order to obtain the services and products that Apria offers.

66. Plaintiff and Class Members had a reasonable expectation and mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access.

67. Plaintiff and Class Members relied on the Defendant to keep their PII and PHI confidential and securely maintained, to use this information for necessary purposes only, and to make only authorized disclosures of this information.

[7] *Id.*

68. Plaintiff and Class Members disclosed their PII and PHI and/or permitted Defendant to collect and store that information in an environment of privacy and confidentiality, and with the reasonable expectation that Defendant would protect that information, entailing Defendant's fiduciary obligations of confidentiality.

69. Plaintiff and Class Members revealed their PII and PHI to Defendant with the understanding, whether express or implicit, that Defendant would keep the information confidential and secure and would not share or disclose it without their explicit authorization and without compliance with HIPAA obligations.

70. Plaintiff and Class Members reasonably relied on Defendant's superior knowledge, skill, and sophistication to safeguard the confidentiality and integrity of their PII and PHI. Indeed, no reasonable person, including Plaintiff and Class Members, would have provided their PII and PHI to Defendant, or allowed Defendant to collect and store such information without an understanding that Defendant would take reasonable steps to protect that information consistent with their representations, their legal obligations, and the implied terms of their express contracts.

The Data Breach

71. As discussed above, although Defendant's systems were breached in both 2019 and 2021, Defendant did not timely notify Plaintiff and Class Members of the Data Breach and/or inform them that their PII and PHI was compromised until May 22, 2023 (the "Notice Letter"), **years** after the Data Breach occurred.

72. Apria confirmed that the hackers gained access to part of its systems and removed copies of personal, medical and financial information of up to 1.8 million individuals.

73. The stolen information included sensitive data including personal, medical records, health insurance information and financial details. The financial data leaked included account numbers, credit/ debit card numbers, account security codes, access codes, passwords and PINs.

As stated by Apria, the "information potentially accessed in the incident varied for each individual and may have included personal, medial, health insurance or financial information, and in some limited cases, Social Security numbers."[8]

74. Plaintiff and other class members received the "Notice Letter" on or about June 25, 2023, stating *inter alia*:

> We are writing to tell you about a data breach that may have exposed some of your personal information. We take the protection and proper use of your information very seriously. For this reason, we are contacting you directly to explain the circumstances of the incident.
>
> **What happened?**
>
> On September 1, 2021, Apria Healthcare LLC ("Apria") received a notification regarding access to select Apria systems by an unauthorized third party. Apria took immediate action to mitigate the incident, including working with the Federal Bureau of Investigation (FBI) and hiring a reputable forensic investigation team to investigate and securely resolve the incident. An unauthorized third party accessed systems which contained personal information from April 5, 2019 to May 7, 2019 and from August 27, 2021 to October 10, 2021.
>
> **What information was involved?**
>
> Based on its investigation and discussions with law enforcement, Apria believes the purpose of the unauthorized access was to fraudulently obtain funds from Apria and not to access personal information of its patients or employees. There is no evidence of funds removed, and Apria is not aware of the misuse of personal information related to this incident. A small number of emails and files were confirmed to have been accessed, but there is no proof that any data was taken from any system. For the individuals receiving this notice, the investigation was unable to confirm whether any emails or files about you were actually accessed. Therefore, Apria has identified the following information relating to you that may have been accessed by the attacker: <>.
>
> **What we are doing.**
>
> Apria has worked with the FBI and forensic investigators to conduct a thorough review of the potentially affected systems. We have also implemented additional security measures upon the guidance and recommendation of our forensic investigators to help prevent the reoccurrence of a similar breach and to further

[8] https://www.apria.com/notice-of-data-breach

> protect the privacy of our patients and employees. To help relieve concerns and restore confidence following this incident, we have secured the services of Kroll to provide identity monitoring at no cost to you for one year. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.
>
> ****
>
> **What you can do.**
>
> Please review the enclosed "Additional Resources" section included with this letter. This section describes additional steps you can take to help protect yourself, including recommendations by the Federal Trade Commission regarding identity theft protection and details on how to place a fraud alert or a security freeze on your credit file.

75. Omitted from the Notice Letter were the details of the root cause of the Data Breach, the vulnerabilities exploited, why it took **years** to inform impacted individuals after Defendant determined its information was involved, and the remedial measures undertaken to ensure such a breach does not occur again. To date, these critical facts have not been explained or clarified to Plaintiff and Class Members, who retain a vested interest in ensuring that their PII and PHI remain protected.

76. Defendant's "disclosure" amounts to no real disclosure at all, as it fails to inform, with any degree of specificity, Plaintiff and Class Members of the Data Breach's critical facts. Without these details, Plaintiff and Class Members' ability to mitigate the harms resulting from the Data Breach is severely diminished.

77. The cyber attackers accessed and acquired files in Defendant's computer systems containing inadequately encrypted or unencrypted PII and PHI of Plaintiff and Class Members, including their names, Social Security numbers, and health and/or clinical information.

Accordingly, Plaintiff and Class Members' PII and PHI was accessed and stolen in the Data Breach.

The Data Breach Was Foreseeable and Preventable

78. Based on the type of customer patient PII and PHI Defendant collects, stores and disseminates, Defendant knows, or should have known, of the likelihood of a ransomware or other cyberattack or data breach of its information technology and data storage systems.

79. Ransomware attacks are frequently used to target healthcare providers due to the sensitive patient data they maintain. Attackers use software to encrypt data on a compromised network, rendering it unusable and demanding payment to restore control over the network. Ransomware attacks are particularly harmful for patients and healthcare providers alike as they cause operational disruptions that result in significant delays in services and accompanying disclosures of PII and PHI.

80. Ransomware attacks must be considered like other data breach incidents because ransomware attacks don't just hold networks hostage. Rather, "ransomware groups sell stolen data in cybercriminal forums and dark web marketplaces for additional revenue." As cybersecurity expert Emisoft warns, "[a]n absence of evidence of exfiltration should not be construed to be evidence of its absence […] the initial assumption should be that data may have been exfiltrated."

81. An increasingly prevalent form of ransomware attack is the "encryption+exfiltration" attack in which the attacker encrypts a network and exfiltrates the data contained within. In 2020, over 50% of ransomware attackers exfiltrated data from a network before encrypting it. Once the data is exfiltrated from a network, its confidential nature is destroyed and it should be "assume[d] it will be traded to other threat actors, sold, or held for a second/future extortion attempt." And even where companies pay for the return of data, attackers often leak or sell the data regardless because there is no way to verify copies of the data are destroyed.

82. The PII and PHI of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, such can be sold at a price ranging from $40 to $200. Criminals can also purchase access to entire company data breaches from $900 to $4,500.

83. Social Security numbers, which were compromised in the Data Breach, are among the worst kind of Private Information to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change.

84. The existence and prevalence of "Fullz" packages means that the PII and PHI stolen from the Data Breach can be linked to unregulated data (like phone numbers and emails) of Plaintiff and the other Class Members, enabling cyber criminals to easily create a comprehensive "Fullz" package. Then, this comprehensive dossier can be sold—and then resold in perpetuity—to crooked operators and other criminals (like illegal and scam telemarketers). This makes the PII and PHI compromised in the Data Breach significantly more valuable than the loss of, for example, credit card information in a retailer data breach because, there, victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change—Social Security numbers, names, and health information.

85. Here, the PII and PHI data Apria collected and maintained demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information, personally identifiable information and Social Security numbers are worth more than 10x on the black market." Accordingly, cyber criminals regularly target healthcare companies, like Defendant, due to the highly sensitive and valuable nature of the information they collect and maintain.

86. Defendant knew and understood that the PII and PHI it collects and maintains is valuable and highly sought after by cyber criminals who seek to illegally monetize that information through unauthorized access and theft.

87. Defendant's data security obligations were particularly important given the substantial increase in cyber-attacks and/or data breaches targeting entities that collect and store PII and PHI, like Defendant, preceding the date of the breach.

88. In 2021, a record 1,862 data breaches occurred, resulting in approximately 293,927,708 sensitive records being exposed, a 68% increase from 2020. The 330 reported breaches reported in 2021 exposed nearly 30 million sensitive records (28,045,658), compared to only 306 breaches that exposed nearly 10 million sensitive records (9,700,238) in 2020.

89. In light of recent high profile cybersecurity incidents at other healthcare partner and provider companies, including American Medical Collection Agency (25 million patients, 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), and BJC Health System (286,876 patients, March 2020), Defendant knew or should have known that its electronic records would be targeted by cybercriminals.

90. Cyber-attacks, such as the one experienced by Defendant, have become so notorious that the Federal Bureau of Investigation ("FBI") and U.S. Secret Service have issued a warning to potential targets so they are aware of, and prepared for, a potential attack. As one report explained, smaller entities that store PII and PHI are "attractive to ransomware criminals…because they often have lesser IT defenses and a high incentive to regain access to their data quickly.

91. As explained by the Federal Bureau of Investigation, "[p]revention is the most effective defense against ransomware and it is critical to take precautions for protection."

92. To prevent and detect cyber/ransomware attack and Data Breach, Defendant could and should have implemented, as recommended by the United States Government, the following measures:

- Implement an awareness and training program. Because end users are targets, employees and individuals should be aware of the threat of ransomware and how it is delivered.

- Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.

- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.

- Configure firewalls to block access to known malicious IP addresses.

- Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system.

- Set anti-virus and anti-malware programs to conduct regular scans automatically.

- Manage the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.

- Configure access controls—including file, directory, and network share permissions—with least privilege in mind. If a user only needs to read specific files, the user should not have write access to those files, directories, or shares.

- Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.

- Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.

- Consider disabling Remote Desktop protocol (RDP) if it is not being used.

- Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.

- Execute operating system environments or specific programs in a virtualized environment.

- Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.

93. To prevent and detect the cyber/ransomware attack and Data Breach, Defendant also could and should have implemented, as recommended by the Microsoft Threat Protection Intelligence Team, the following measures:

Secure internet-facing assets

- Apply latest security updates
- Use threat and vulnerability management
- Perform regular audit; remove privileged credentials;

Thoroughly investigate and remediate alerts

- Prioritize and treat commodity malware infections as potential full compromise;

Include IT Pros in security discussions

- Ensure collaboration among [security operations], [security admins], and [information technology] admins to configure servers and other endpoints securely;

Build credential hygiene

- Use [multifactor authentication] or [network level authentication] and use strong, randomized, just-in-time local admin passwords;

Apply principle of least-privilege

- Monitor for adversarial activities
- Hunt for brute force attempts
- Monitor for cleanup of Event Logs
- Analyze logon events;

Harden infrastructure

- Use Windows Defender Firewall
- Enable tamper protection
- Enable cloud-delivered protection
- Turn on attack surface reduction rules and [Antimalware Scan Interface] for Office[Visual Basic for Applications].

94. Had Defendant adequately and fully implemented the above-described data security protocols, policies, and/or procedures, the consequences of the Data Breach could have been avoided or greatly reduced.

95. Defendant could have prevented or detected the Data Breach prior to the hackers accessing Defendant's systems and extracting sensitive and personal information; the amount and/or types of PII accessed by the hackers could have been avoided or greatly reduced; and current and former patients of Defendant would have been notified sooner, allowing them to promptly take protective and mitigating actions.

96. Upon information and belief, Defendant did not use reasonable security procedures and practices appropriate to the nature of the sensitive information it was maintaining for Plaintiff and Class Members, causing the exposure of PII and PHI, such as encrypting the information or deleting it when it is no longer needed.

97. Upon information and belief, Defendant did not comply with HIPAA, FTC or cybersecurity industry standards to protect its customer patients' PII and/or PHI, including such information of Plaintiff and Class Members.

98. But for Defendant's failures, Plaintiff's and Class Members' PII and PHI would not have been exposed to the Data Breach and stolen.

PLAINTIFF'S EXPERIENCE WITH DEFENDANT

99. Plaintiff Rabinovich operates a private business in the automotive industry. Given his automotive finance-related knowledge, he is highly knowledgeable about the importance of preventing unauthorized access to an individuals' social security number and credit file.

100. Over the last fifteen years or so, Plaintiff Rabinovich obtained personal medical supply materials from Apria for his health issues, using his Medicare insurance through which Defendant was necessarily provided with his PII and PHI and which Defendant maintained in the ordinary course of its business.

101. At the time of the Data Breach, Defendant was in the possession, custody and control of Plaintiff Rabinovich's PII and PHI data in its computer system.

102. Plaintiff Rabinovich is, and has been, very careful about sharing any of his PII and PHI, stores any documents containing his PII and PHI in a safe and secure location and has never knowingly transmitted unencrypted PII or PHI to any unauthorized third party or over the internet or any other unsecured source.

103. Plaintiff Rabinovich is concerned that his social security number and medical information has been compromised. He is concerned that his HIPAA rights were violated and is incredibly concerned about the security of his credit and financial information.

104. On or about June 25, 2023, Mr. Rabinovich received Apria's Notice Letter by U.S. mail. The Notice Letter did not provide any details of what specific information was taken from him.

105. Following Defendant's Data Breach, Mr. Rabinovich suffered a number of direct injuries. For example, an unknown party residing in Dubai, U.A.E., recently applied for, and attempted to obtain, a replacement American Express card using Mr. Rabinovich's PII information. In addition, an unauthorized person attempted to obtain a second mortgage on his

home. Shortly thereafter, Mr. Rabinovich learned of an unauthorized wire transfer in the amount $24,850 from his business account that Mr. Rabinovich was unable to stop. At the time, Mr. Rabinovich was told by his bank that "he had called them," which he did not, and that he would send "his business partner to complete the wire transfer request," which he did not.

106. Plaintiff Rabinovich suffered actual injury from having his PII and PHI compromised as a result of the Data Breach including, but not limited to: (i) invasion of his privacy; (ii) loss of benefit of his bargain with Defendant when using its medical/laboratory services/products; (iii) lost time he 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; (v) diminished value to his PII; and (vi) the continued and certainly increased risk to his PII and PHI, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains 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 his PII and PHI.

107. As a result of the Data Breach, and at the direction of Defendant's Notice Letter, Plaintiff Rabinovich has made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to: researching the Data Breach to verify the incident, speaking with his credit card companies and other lenders to try to stop any credit applications in his name, locking his credit file, communicating with his business' bank to try to stop the unauthorized wire, contacting credit reporting agencies, and numerous efforts to change his passwords on his social media and email accounts.

108. Plaintiff Rabinovich has spent at least 25 hours of his time on his efforts to mitigate his concrete injuries from the data breach—valuable time Plaintiff otherwise would have spent on

other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

109. Plaintiff Rabinovich is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come. Accordingly, Plaintiff Rabinovich anticipates spending considerable additional time and money on an ongoing basis to try to mitigate and address future harms caused by the Data Breach.

110. The Data Breach has caused Plaintiff Rabinovich to suffer anxiety and stress, including his fear of additional unknown repercussions, all of which has been compounded by the fact that Defendant has still not fully informed him of the key details about the Data Breach's occurrence or bothered to offer him credit monitoring.

111. Plaintiff Rabinovich has a continuing interest in ensuring that his PII and PHI, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

PLAINTIFF'S AND CLASS MEMBERS' COMMON INJURIES

112. As a result of the Data Breach and Defendant's related failures to adequately protect its customer patients' PII and PHI information, Plaintiff and Class Members have all sustained actual injuries and damages, including: (a) invasion of privacy; (b) "out of pocket" costs incurred mitigating the materialized risk and imminent threat of identity theft; (c) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft risk; (d) loss of time incurred due to actual identity theft; (e) loss of time due to increased spam and targeted marketing emails; (f) the loss of benefit of the bargain (price premium damages); (g) diminution of value of their PII; and (i) the continued risk to their PII and PHI, which remain in the possession of Defendant, and which is subject to further breaches, so long as Defendant fails to undertake

appropriate and adequate measures to protect Plaintiff's and Class Members' confidential information.

113. The link between a data breach and the risk of identity theft is simple and well established. Criminals acquire and steal Private Information to monetize the information. Criminals monetize the data by selling the stolen information on the black market to other criminals who then utilize the information to commit a variety of identity theft related crimes.

114. The unencrypted PII and PHI of Plaintiff and Class Members will be available for sale on the dark web as that is the *modus operandi* of hackers, as already has been experienced by Plaintiff.

115. Unencrypted PII and PHI of Plaintiff and Class Members may also fall into the hands of unauthorized individuals and companies that will use such information for targeted marketing without the approval of Plaintiff and Class Members.

116. As a consequence of the Data Breach, Plaintiff and Class Members must take time to learn about the breach and are expected to take reasonable steps to mitigate injuries including, but not limited to, researching the Data Breach to verify the incident and obtain more details on its occurrence, monitoring their financial accounts and monitoring their credit files with the credit reporting agencies, contacting one of the credit bureaus to place a fraud alert, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.

117. According to a 2022 Consumer Impact Report by the Identity Theft Resource Center, available at https://www.idtheftcenter.org/publications/, victims of data breaches/cyber theft have experienced numerous types of harm, including financial injuries, the expenditure of time to resolve id theft and credit issues, and emotional/psychological injuries, with total financial value of such injuries exceeding $500 for 65% of all victims.

118. Given the nature and extent of PII and PHI data Apria collects, stores and disseminates for its customer patients, there is a strong probability that entire batches of stolen information have been placed, or will be placed, on the black market/dark web for sale and purchase by criminals intending to utilize Plaintiff's and Class Members' PII and PHI for identity theft crimes, including, e.g., opening credit cards or taking out loans in their name; filing false income tax returns and intercepting refunds; and filing false unemployment claims.

119. Such fraud may go undetected until debt collection calls commence months, or even years, later. An individual may not know that his or his Private Information 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.

120. Because fraudulent activity involving Plaintiff's and Class Members' PII and PHI resulting from the Data Breach may not come to light for years, Plaintiff and Class Members will be required to maintain constant surveillance of their financial and personal records for years to come.

121. In addition, Plaintiff's and Class Members' rights to their PII and PHI are valuable property rights. Sensitive PII can sell for as much as $363 per record according to the Infosec Institute.

122. An active and robust legitimate marketplace for PII exists. In 2019, the data brokering industry was worth roughly $200 billion. The data marketplace even enables consumers to sell their non-public information to data brokers who in turn aggregate such information and re-sell it to marketers and app developers, including the Nielsen Corporation.

123. As a result of the Data Breach, Plaintiff's and Class Members' PII, which has an inherent market value in both legitimate and dark markets, has been damaged and diminished by

its compromise and unauthorized release. This transfer of value occurred without any consideration paid to Plaintiff or Class Members for their property, resulting in an economic loss. Moreover, their PII is now readily available, and the rarity of the data has been lost, thereby causing additional loss of value.

124. Plaintiff and Class Members will need credit and identity theft monitoring for a minimum of five years to protect their identities as a result of the Data Breach. The retail cost of such monitoring can run approximately $200 a year per Class Member. Such costs are reasonable and necessary to protect Class Members from the risk of identity theft.

125. Defendant's failure to protect Plaintiff's and Class Members' PII and PHI deprived them of the benefit of their bargain with Defendant when paying for Defendant's medical and laboratory products and services.

126. When agreeing to pay Defendant for such medical and laboratory services and products, Plaintiff and Class Members understood and expected that they were, in part, paying for the service and necessary data security to protect their PII and PHI, when in fact, Defendant did not provide the expected data security. Accordingly, the products and services that Plaintiff and Class Members received from Defendant were of a lesser value than what they reasonably expected to receive under the bargains they struck with Defendant.

CLASS ACTION ALLEGATIONS

127. Plaintiff brings this action on behalf of himself and on behalf of all other persons similarly situated.

128. Pursuant to Federal Rule of Civil Procedure 23, Plaintiff proposes the following Class definition, subject to amendment as appropriate:

> All persons whose PII and/or PHI was maintained on Defendant's computer systems that were compromised in the Data Breach reported by Defendant in May 2023 (the "Class").

129. Excluded from the Class are Defendant, officers and directors, and any entity in which Defendant has a controlling interest; and the affiliates, legal representatives, attorneys, successors, heirs, and assigns of Defendant. Excluded also from the Class are members of the judiciary to whom this case is assigned, their families and members of their staff.

130. Plaintiff hereby reserves the right to amend or modify the Class definition with greater specificity or division after having had an opportunity to conduct discovery.

131. Numerosity. The Members of the Class are so numerous that joinder of all of them is impracticable. While the exact number of Class Members is unknown to Plaintiff at this time, it has been reported that the Class consists of approximately 1.8 million persons whose data was compromised in the Data Breach.

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

a. Whether Defendant unlawfully used, maintained, provided access to, or disclosed Plaintiff's and Class Members' PII and PHI;

b. Whether Defendant failed to implement and maintain reasonable and adequate security procedures and practices appropriate to the nature and scope of the PII and PHI compromised in the Data Breach;

c. Whether Defendant's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

d. Whether Defendant's data security systems prior to and during the Data Breach were consistent with industry standards;

e. Whether Defendant owed a duty to Plaintiff and Class Members to safeguard their PII and PHI;

f. Whether Defendant breached its duties to Plaintiff and Class Members to safeguard their PII and PHI;

g. Whether computer hackers obtained Plaintiff's and Class Members' PII and PHI in the Data Breach;

h. Whether Defendant knew or should have known that its data security systems and monitoring processes were deficient;

i. Whether Plaintiff and Class Members suffered legally cognizable damages as a result of Defendant's misconduct;

j. Whether Defendant's conduct was negligent;

k. Whether Defendant breached implied contracts for adequate data security with Plaintiff and Class Members;

l. Whether Defendant was unjustly enriched by retention of the monetary benefits conferred on it by Plaintiff and Class Members;

m. Whether Defendant failed to provide adequate notice of the Data Breach in a timely manner; and,

n. Whether Plaintiff and Class Members are entitled to damages, civil penalties, punitive damages, and/or injunctive relief.

146. Typicality. Plaintiff's claims are typical of those of other Class Members because Plaintiff's PII and PHI, like that of every other Class Member, was compromised in the Data Breach.

147. Adequacy of Representation. Plaintiff will fairly and adequately represent and protect the interests of the Members of the Class. Plaintiff's Counsel is competent and experienced in litigating class actions.

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

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

150. Defendant has acted on grounds that apply generally to the Class as a whole, so that class certification, injunctive relief, and corresponding declaratory relief are appropriate on a class-wide basis.

151. Likewise, particular issues under Fed. R. Civ. P. 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendant owed a legal duty to Plaintiff and the Class Members to exercise due care in collecting, storing, and safeguarding their PII and PHI;

b. Whether Defendant's security measures to protect its data systems were compliant with HIPAA and FTC requirements;

c. Whether Defendant's security measures to protect its data systems were reasonable in light of best practices recommended by data security experts;

d. Whether Defendant failed to take reasonable and appropriate steps to safeguard Plaintiff's and Class Members' PII and PHI;

e. Whether Defendant's failure to institute adequate protective security measures amounted to negligence; and

f. Whether adherence to FTC data security recommendations, and measures recommended by data security experts would have reasonably prevented the Data Breach.

152. Finally, all Members of the proposed Class are readily ascertainable. Defendant has access to Class Members' names and addresses affected by the Data Breach. Class Members have already been preliminarily identified and sent Notice of the Data Breach by Defendant.

CAUSES OF ACTION

Count I – Negligence
(On Behalf of Plaintiff and All Class Members)

153. Plaintiff re-alleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

154. Defendant requires their customers and clients, including Plaintiff and Class Members, to submit non-public PII and PHI in the ordinary course of providing its medical/laboratory products and services.

155. Defendant gathered and stored the PII and PHI of Plaintiff and Class Members as part of its business of soliciting its services to its clients and its clients' patients, which solicitations and services affect commerce.

156. Plaintiff and Class Members entrusted Defendant with their PII and PHI with the understanding that Defendant would safeguard their information.

157. Defendant had full knowledge of the sensitivity of Plaintiff's and Class Members' PII and PHI, as well as the types of harm that Plaintiff and Class Members could and would suffer if their PII and PHI were wrongfully disclosed.

158. 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 its computer property—and Class Members' PII and PHI held within it—to prevent unauthorized access and 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.

159. 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.

160. 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.

161. Defendant owed a duty of care to Plaintiff 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 PII and PHI.

162. Defendant's duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendant and its customer patients. That special relationship arose because Plaintiff and the Class Members entrusted Defendant with their confidential PII and PHI, a necessary part of being customer patients of Defendant.

163. 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 PII and PHI.

164. Defendant was subject to an "independent duty," untethered to any contract between Defendant and Plaintiff or the Class Members.

165. Defendant also had a duty to exercise appropriate clearinghouse practices to remove former customer patients' PII and PHI that it was no longer required to retain pursuant to regulations.

166. Defendant had a duty to promptly and adequately notify Plaintiff and the Class of the Data Breach.

167. Defendant had and continues to have a duty to adequately disclose that the PII and PHI of Plaintiff and Class Members 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 is necessary to allow Plaintiff and Class Members to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their confidential information by third parties.

168. Defendant breached its duties, pursuant to the FTC Act, HIPAA, and other applicable standards, and thus were negligent, by failing to use reasonable measures to protect Plaintiff's and Class Members' PII and PHI. 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 Plaintiff's and Class Members' PII and PHI;

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

c. Allowing unauthorized access to, and the theft of, Plaintiff's and Class Members' PII and PHI;

d. Failing to detect in a timely manner that Plaintiff's and Class Members' PII and PHI had been compromised;

e. Failing to remove former customer patients' PII and PHI it was no longer required to retain pursuant to regulations, and

f. Failing to timely and adequately notify Plaintiff and 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.

169. Defendant violated Section 5 of the FTC Act and HPAA by failing to use reasonable measures to protect Plaintiff's and Class Members' PII and PHI and not complying with applicable industry standards, as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of PII and PHI it obtains, stores and disseminates in the ordinary course of its business and the foreseeable consequences of the immense damages that would result to Plaintiff and Class Members if that data was accessed and stolen.

170. Plaintiff and Class Members are within the class of persons that the FTC Act and HIPAA were intended to protect.

171. 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.

172. Defendant's violation of Section 5 of the FTC Act and HIPAA constitutes negligence.

173. A breach of security, unauthorized access, and resulting injury to Plaintiff and the Class Members was reasonably foreseeable, particularly in light of the nature of Defendant's business and its inadequate security practices.

174. It was foreseeable that Defendant's failure to use reasonable measures to protect Plaintiff's and Class Members' PII and PHI 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 the healthcare industry.

175. Defendant has full knowledge of the sensitivity of the PII and PHI and the types of harm that Plaintiff and Class Members could and would suffer if their PII and PHI were wrongfully disclosed.

176. Plaintiff and the Class were the foreseeable and probable victims of any inadequate security practices and procedures.

177. Defendant knew or should have known of the inherent risks in collecting and storing the PII and PHI of Plaintiff and the Class, the critical importance of providing adequate security of that information, and the necessity for encrypting such information stored on Defendant's computer systems and network.

178. It was therefore foreseeable that the failure to adequately safeguard Plaintiff's and Class Members' PII and PHI would result in one or more types of injuries to Plaintiff and Class Members.

179. Plaintiff and Class Members had no ability to protect their PII and PHI that was in, and possibly remains in, Defendant's possession.

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

181. Defendant's duty extended to protecting Plaintiff and Class Members 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.

182. Defendant has admitted that the PII and PHI of Plaintiff and Class Members were wrongfully accessed by cybercriminals and potentially lost and disclosed to unauthorized third persons as a result of the Data Breach.

183. But for Defendant's wrongful and negligent breach of duties owed to Plaintiff and Class Members, the PII and PHI of Plaintiff and Class Members would not have been compromised.

184. There is a close causal connection between Defendant's failure to implement security measures to protect the PII and PHI of Plaintiff and Class Members and the harm, or risk of imminent harm, suffered by Plaintiff and Class Members. The PII and PHI of Plaintiff and the Class Members were accessed and stolen as the proximate result of Defendant's failure to exercise reasonable care in safeguarding such information by adopting, implementing, and maintaining appropriate security measures.

185. As a direct and proximate result of Defendant's negligence, Plaintiff and the Class Members have suffered and will suffer injury, 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; (v) the diminished value of their PII and PHI, and (vi) the continued and certainly increased risk to their PII and PHI, 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 that information.

186. As a direct and proximate result of Defendant's negligence, Plaintiff 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.

187. Additionally, as a direct and proximate result of Defendant's negligence, Plaintiff and Class Members have suffered and will suffer the continued risks of exposure of their PII and PHI, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect such information in their continued possession.

188. Defendant's negligent conduct is ongoing, in that it still holds the PII and PHI of Plaintiff and Class Members in an unsafe and insecure manner.

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

190. Plaintiff and Class Members also are 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 – Breach of Implied Contract
(On Behalf of Plaintiff and All Class Members)

191. Plaintiff re-alleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

192. Plaintiff and Class Members were required to provide their PII and PHI to Defendant as a condition of, and a necessary part of, receiving medical/laboratory products and services from Defendant.

193. Plaintiff and Class Members entrusted their PII and PHI to Defendant. In so doing, Plaintiff and Class Members entered into implied contracts with Defendant by which Defendant

agreed to safeguard and protect such information, to keep such information secure and confidential, and to timely and accurately notify Plaintiff and Class Members if their data had been breached and compromised or stolen.

194. Implicit in the agreement between Plaintiff and Class Members on the one hand, and the Defendant on the other hand, to provide their PII and PHI, Defendant was obligated to: (a) use such PII and PHI for authorized business purposes only, (b) take reasonable steps to safeguard that information, (c) prevent unauthorized disclosures of the information, (d) provide Plaintiff and Class Members with prompt and sufficient notice of any and all unauthorized access and/or theft of their PII and PHI, (e) reasonably safeguard and protect the PII and PHI of Plaintiff and Class Members from unauthorized disclosure or uses, and (f) retain the PII and PHI only under conditions that kept such information secure and confidential.

195. The mutual understanding and intent of Plaintiff and Class Members on the one hand, and Defendant, on the other, is demonstrated by their conduct and course of dealing.

196. Defendant solicited, offered, and invited Plaintiff and Class Members to provide their PII and PHI, and enable Defendant to collect, maintain and disseminate such information, as part of Defendant's regular business practices. Plaintiff and Class Members accepted Defendant's offers and provided their PII and PHI to Defendant.

197. In accepting the PII and PHI of Plaintiff and Class Members, Defendant understood and agreed that it was required to reasonably safeguard that information from unauthorized access or disclosure.

198. At all relevant times Defendant promulgated, adopted, and implemented written privacy policies whereby it expressly promised Plaintiff and Class Members that it would only disclose PII and PHI under certain circumstances, none of which relate to the Data Breach.

199. Defendant implicitly promised to comply with industry standards and to make sure that Plaintiff's and Class Members' PII and PHI would remain protected.

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

201. Plaintiff and Class Members paid money to Defendant with the reasonable belief and expectation that Defendant would use part of its earnings to obtain adequate data security. Defendant failed to do so.

202. Plaintiff and Class Members would not have entrusted their PII and PHI to Defendant in the absence of the implied contract between them and Defendant to keep their information reasonably secure.

203. Plaintiff and Class Members would not have entrusted their PII and PHI to Defendant in the absence of Defendant's implied promise to monitor its computer systems and networks to ensure that it adopted reasonable data security measures.

204. Plaintiff and Class Members fully and adequately performed their obligations under the implied contracts with Defendant.

205. Defendant breached the implied contracts it made with Plaintiff and Class Members by failing to safeguard and protect their PII and PHI, by: (a) failing to delete such information once the relationship ended, and (b) by failing to provide adequate notice to them that personal information was compromised as a result of the Data Breach.

206. As a direct and proximate result of Defendant's breach of the implied contracts, Plaintiff and Class Members sustained damages, as alleged herein, including the loss of the benefit of the bargain.

207. Plaintiff and Class Members are entitled to compensatory, consequential, and nominal damages suffered as a result of the Data Breach.

Count III – Unjust Enrichment
(On Behalf of Plaintiff and All Class Members)

208. Plaintiff re-alleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

209. Plaintiff and Class Members conferred a monetary benefit on Defendant. Specifically, they paid for services from Defendant and/or their agents and in so doing provided Defendant with their PII and PHI. In exchange, Plaintiff and Class Members should have received from Defendant the medical/laboratory services and products that were the subject of the transaction and should have had their PII and PHI protected with adequate data security.

210. Defendant knew that Plaintiff and Class Members conferred a benefit on it in the form of their PII and PHI, as well as payments made on their behalf as a necessary part of their receiving healthcare services and products. Defendant appreciated and accepted that benefit. Defendant profited from these transactions and used the PII and PHI of Plaintiff and Class Members for business purposes.

211. 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 the medical/laboratory products and services that Defendant provides to Plaintiff and Class Members.

212. As such, a portion of the payments made for the benefit of or on behalf of Plaintiff 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.

213. Defendant, however, failed to secure Plaintiff's and Class Members' PII and PHI and, therefore, did not provide adequate data security in return for the benefit Plaintiff and Class Members provided to Defendant.

214. Defendant would not be able to carry out an essential function of their regular business without the PII and PHI of Plaintiff and Class Members and derived revenue by using that information for its business purposes. Plaintiff 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.

215. Defendant acquired the PII and PHI through inequitable means in that it failed to disclose the inadequacy of its security practices to Plaintiff and Class Members. If Plaintiff and Class Members knew that Defendant had not reasonably secured their PII and PHI, they would not have allowed their PII and PHI to be provided to Defendant.

216. Defendant enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiff's and Class Members' PII and PHI. Instead of providing a reasonable level of security that would have prevented the hacking incident, Defendant instead calculated to increase its own profit at the expense of Plaintiff and Class Members by utilizing cheaper, ineffective security measures and diverting those funds to its own profit. Plaintiff and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's decision to prioritize its own profits over the requisite security and the safety of their PII and PHI.

217. Under the principles of equity and good conscience, Defendant should not be permitted to retain the money wrongfully obtained from Plaintiff and Class Members because Defendant failed to implement appropriate data management and security measures that are mandated by industry standards.

218. Plaintiff and Class Members have no adequate remedy at law.

219. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will suffer injury, 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; (v) diminished value of their PII; and (vi) 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 Plaintiff's and Class Members' PII and PHI.

220. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm.

221. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and Class Members, proceeds that they unjustly received from them. In the alternative, Defendant should be compelled to refund the amounts that Plaintiff and Class Members overpaid for Defendant's products and services.

PRAYER FOR RELIEF

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

A. For an Order certifying this action as a class action and appointing Plaintiff and his counsel to represent the Class, pursuant to Federal Rule of Civil Procedure 23;

B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and

Class Members' PII and PHI, and from refusing to issue prompt, complete and accurate disclosures to Plaintiff and Class Members;

C. For injunctive relief requested by Plaintiff, including, but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and Class Members, including but not limited to an order:

i. prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;

ii. requiring Defendant to protect, including through encryption, all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state or local laws;

iii. requiring Defendant to delete, destroy, and purge the PII and PHI of Plaintiff and Class Members unless Defendant can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and Class Members;

iv. requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the PII and PHI of Plaintiff and Class Members;

v. prohibiting Defendant from maintaining the PII and PHI of Plaintiff and Class Members on a cloud-based database;

vi. requiring Defendant 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 Defendant's computer systems and network on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

vii. requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring;

viii. requiring Defendant to audit, test, and train their security personnel regarding any new or modified procedures;

ix. requiring Defendant to segment data by, among other things, creating firewalls and access controls so that if one area of Defendant's

network is compromised, hackers cannot gain access to other portions of Defendant's computer systems

x. requiring Defendant to conduct regular database scanning and securing checks;

xi. requiring Defendant 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 PII and PHI of Plaintiff and Class Members;

xii. requiring Defendant 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;

xiii. requiring Defendant 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 Defendant's policies, programs, and systems for protecting personal identifying information;

xiv. requiring Defendant to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendant's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

xv. requiring Defendant 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;

xvi. requiring Defendant to implement logging and monitoring programs sufficient to track traffic to and from Defendant's servers; and

xvii. 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 Defendant's compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the Class Members, 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.

Dated: July 7, 2023

Respectfully submitted,

s/ Sandra L. Blevins

Sandra L. Blevins, Atty. No. 19646-49
Jamie A. Maddox, Atty. No. 26522-49
BETZ + BLEVINS
One Indiana Square, Suite 1660
Indianapolis, Indiana 46204
Office: (317) 687-2222
Fax: (317) 687-2221
E-mail: sblevins@betzadvocates.com
jmaddox@betzadvocates.com
litigation@betzadvocates.com

James M. Evangelista
EVANGELISTA WORLEY LLC
500 Sugar Mill Road
Suite 245A
Atlanta, GA 30350
Tel.: 404-205-8400
Fax: 404-205-8395
Email: jim@ewlawllc.com

Jennifer Czeisler
JKC LAW, LLC
269 Altessa Blvd.
Melville, NY 11747
Tel: (516)457-9571
Email: jennifer@jkclawllc.com

Attorneys for Plaintiff

JS 44 (Rev. 10/20)

CIVIL COVER SHEET

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

I. (a) PLAINTIFFS

ILYA RABINOVICH

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

(c) Attorneys *(Firm Name, Address, and Telephone Number)*

Sandra L. Blevins, Betz + Blevins, 317-687-2222
1 Indiana Sq. Ste 1660, Indianapolis, IN 46204

DEFENDANTS

APRIA HEALTHCARE,LLC

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

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

Attorneys *(If Known)*

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

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

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

(For Diversity Cases Only)

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

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

Click here for: Nature of Suit Code Descriptions.

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

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

TORTS

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

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

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

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

PRISONER PETITIONS

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

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

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

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

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

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

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

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

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

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

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

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

VI. CAUSE OF ACTION

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

Brief description of cause:
Class Action Complaint for Negligence, Implied Breach of Contract and Unjust Enrichment

VII. REQUESTED IN COMPLAINT:

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

DEMAND $ $5,000,000+

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

VIII. RELATED CASE(S) IF ANY

(See instructions): JUDGE _____ DOCKET NUMBER _____

DATE July 7, 2023

SIGNATURE OF ATTORNEY OF RECORD s/ Sandra L. Blevins

FOR OFFICE USE ONLY

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

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

UNITED STATES DISTRICT COURT

for the

Southern District of Indiana

Ilya Rabinovich

Plaintiff(s)

v.

Apria Healthcare LLC

Defendant(s)

Civil Action No. 1:23-cv-1205

SUMMONS IN A CIVIL ACTION

To: *(Defendant's name and address)* Apria Healthcare LLC
Business Commercial Registered Agent
NATIONAL REGISTERED AGENTS, INC.
334 North Senate Avenue, Indianapolis, IN 46204, USA

A lawsuit has been filed against you.

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

Sandra L. Blevins, Esquire
Jamie A. Maddox, Esquire
Betz + Blevins
One Indiana Square, Suite 1660
Indianapolis, IN 46204

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

CLERK OF COURT

Date: _____

_____
Signature of Clerk or Deputy Clerk

Civil Action No. 1:23-cv-1205

PROOF OF SERVICE

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

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

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

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

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

❒ I returned the summons unexecuted because _____ ; or

❒ Other *(specify):*

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

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

Date: _____

_____
Server's signature

_____
Printed name and title

_____
Server's address

Additional information regarding attempted service, etc: