IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF ARKANSAS

NICHOLAS BURGESS, individually and on behalf of all others similarly situated,

Plaintiff,

v.

ARISA HEALTH, INC.,

Defendant.

Case No.:

CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

PLAINTIFF'S ORIGINAL CLASS ACTION COMPLAINT AND JURY DEMAND

Plaintiff Nicholas Burgess, individually and on behalf of all others similarly situated, sues Defendant Arisa Health, Inc. to obtain damages, restitution, and injunctive relief for the Class, as defined below, from Defendant. Plaintiff makes the following allegations upon information and belief, except as to his own actions, the investigation of his counsel, and the facts that are a matter of public record.

I. INTRODUCTION

1. This class action arises out of the recent data security incident and data breach that was perpetrated against Defendant (the "Data Breach"), which held in its possession certain personally identifiable information ("PII") and protected health information ("PHI") (collectively, the "Private Information") of Plaintiff and other current and former patients of Defendant, the putative class members ("Class"). This Data Breach occurred between March 1-18, 2024.

2. The Private Information compromised in the Data Breach included certain personal or protected health information of Defendant Arisa Health, Inc.'s ("Arisa" or "Defendant") customers, employees, and patients, including Plaintiff. This Private Information included but is

not limited to "full name, address, date of birth, email address, Social Security number, medical record number, health insurance number or member ID, certification of substance abuse program completion, medical history and diagnosis, and driver's license number."[1]

3. The Private Information was "accessed and/or acquired" by cyber-criminals who perpetrated the attack and remains in the hands of those cyber-criminals. According to Defendant's report to the Office of the Attorney General of Texas, 1,434 or more Texans Sensitive Data was compromised.[2]

4. The Data Breach resulted from Defendant's failure to implement adequate and reasonable cyber-security procedures and protocols necessary to protect individuals' Private Information with which they were entrusted for either treatment or employment or both.

5. Plaintiff brings this class action lawsuit on behalf of those similarly situated to address Defendant's inadequate safeguarding of Class Members' Private Information that they collected and maintained, and for failing to provide timely and adequate notice to Plaintiff and other Class Members that their information was subjected to unauthorized access by an unknown third party and precisely what specific type of information was accessed.

6. Defendant maintained the Private Information in a reckless manner. In particular, the Private Information was maintained on Defendant's computer network in a condition vulnerable to cyberattacks. Upon information and belief, the mechanism of the Data Breach and potential for improper disclosure of Plaintiff's and Class Members' Private Information was a known risk to Defendant, and thus Defendant was on notice that failing to take steps necessary to secure the Private Information from those risks left that property in a dangerous condition.

---

[1] Defendant Arisa Health, Inc., *Notice of Data Security Incident* (July 19, 2024), *available at* https://www.arisahealth.org/notice-of-data-security-incident (*last accessed* July 29, 2024).

[2] Office of the Attorney General of Texas, *Data Security Breach Reports* (July 22, 2024), *available at* https://oag.my.site.com/datasecuritybreachreport/apex/DataSecurityReportsPage (*last accessed* July 29, 2024).

7. Defendant, through its employees, disregarded the rights of Plaintiff and Class Members (defined below) by, among others, intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure its data systems were protected against unauthorized intrusions. Defendant also failed to disclose that it did not have adequately robust computer systems and security practices to safeguard Plaintiff's and Class Members' Private Information and failed to take standard and reasonably available steps to prevent the Data Breach.

8. In addition, Defendant's employees failed to properly monitor the computer network and systems that housed the Private Information. Had Defendant's employees (presumably in the IT department) properly monitored its property, it would have discovered the intrusion sooner.

9. Plaintiff's and Class Members' identities are now at risk because of Defendant's negligent conduct since the Private Information that Defendant collected and maintained is now in the hands of data thieves.

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

11. Because of the Data Breach, Plaintiff and Class Members have been exposed to a heightened and imminent risk of fraud and identity theft. Plaintiff and Class Members must now and in the future closely monitor their financial accounts to guard against identity theft.

12. Plaintiff and Class Members may also incur out of pocket costs for, *e.g.*, purchasing credit monitoring services, credit freezes, credit reports, or other protective measures to deter and detect identity theft.

13. Through this Complaint, Plaintiff seeks to remedy these harms on behalf of himself and all similarly situated individuals whose Private Information was accessed during the Data Breach.

14. Plaintiff seek remedies including, but not limited to, compensatory damages, reimbursement of out-of-pocket costs, and injunctive relief including improvements to Defendant's data security systems, future annual audits, and adequate credit monitoring services funded by Defendant.

15. Accordingly, Plaintiff sue Defendant seeking redress for their unlawful conduct, and asserting claims for: (i) negligence, (ii) negligence *per se*, (iii) breach of implied contract, (iv) breach of fiduciary duty; (v) unjust enrichment; and (vi) declaratory judgment.

II. PARTIES

16. Plaintiff Nicholas Burgess is and at all times mentioned herein was an individual citizen of Arkansas, residing in the city of Mayflower.

17. Plaintiff provided Defendant with his sensitive PII and PHI to receive behavioral care services from providers working with Defendant. Plaintiff received notice of the Data Breach around July 19, 2024, informing his that his sensitive information was part of Defendant's Data Breach, including his "Address, date of birth, email address, Social Security number, medical record number, health insurance number, medical history and diagnosis, and driver's license number"—which includes PHI. A copy of the letter is attached **Exhibit A**.

18. Plaintiff reasonably expected and understood that Defendant would take, at a minimum, industry standard precautions to protect, maintain, and safeguard his Private

Information from unauthorized users or disclosure, and would timely notify his of any data security incidents related to the same. Plaintiff would not have provided his Private Information to Defendant had he known that Defendant would not take reasonable steps to safeguard it.

19. Plaintiff is very careful about sharing his sensitive PII and PHI. He has never knowingly transmitted unencrypted sensitive PII or PHI over the internet or any other unsecured source. Plaintiff also stores any documents containing his sensitive information in a safe and secure location or destroys the documents. Moreover, he diligently chooses unique usernames and passwords for his various online accounts.

20. Because of the Data Breach and at the recommendation of Defendant and its Notice, Plaintiff made reasonable efforts to mitigate the effect of the Data Breach, including, but not limited to, researching the Data Breach, reviewing financial statements, monitoring his credit information, and changing passwords on his various accounts.

21. Plaintiff has spent much time responding to the dangers from the Data Breach and will continue to spend valuable time he otherwise would have spent on other activities, including, but not limited to work and recreation.

22. Defendant Arisa Health, Inc. is an Arkansas based entity that medical services in the form of behavioral care. Defendant's principal place of business is 2400 S. 48th Street Springdale, AR 72762, that operates nationally. Its registered agent is Rayburn W. Green, located at 3356 East Chatsworth Road Fayetteville, AR 72703.

23. Arisa is sued both directly and vicariously based on respondeat superior liability under state law, as it is responsible for the actions of all its agents and employees performed in the course and scope of their employment and/or agency. All the actions alleged here by agents and employees of Arisa were so performed. Thus, Arisa is liable for the actions of all its employees

and agents, named or unnamed, who performed acts at issue in this lawsuit, all of whom were acting in the course and scope of their employment and/or agency. The actions alleged here were undertaken by Arisa by custom and policy of those entities, making it independently liable under federal law.

III. JURISDICTION AND VENUE

24. This court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5,000,000, exclusive of interest and costs. Upon information and belief, the number of class members is at least 1,434, all of whom have different citizenship from Defendant.[3] Thus, minimal diversity exists under 28 U.S.C. § 1332(d)(2)(A).

25. This Court has general personal jurisdiction over Defendant because it is an entity based and operating in this District and the acts and omissions giving rise to Plaintiff's claims occurred in and emanated from this District.

26. Venue is proper in this District under 28 U.S.C. §§ 1391(a)(2), 1391(b)(2), and 1391(c)(2) because Defendant maintains its principal place of business within the Western District of Arkansas and because a substantial part of the acts or omissions giving rise to this action occurred within this District.

IV. THE FEDERAL TORT CLAIMS ACT'S IMMUNITY IS INAPPLICABLE

27. Plaintiff's claims are not brought "for damage for personal injury, including death, resulting from the performance of medical, surgical, dental, or related functions." *Marshall v. Lamoille Health Partners, Inc.*, No. 2:22-CV-166, 2023 WL 2931823, at *1 (D. Vt. Apr. 13, 2023) (finding no data breach "technology-related activities were 'interwoven' with the provision of

[3] *Id.*

medical care" in analogous case). Thus, though Defendant may claim it is immune to data breach claims under the Federal Tort Claims Act (FTCA), the Office of the General Counsel of the U.S. Department of Health and Human Services agrees that such claims fall outside the immunity provided under the FTCA. *Id*. at *1.

28. The FTCA's "legislative history … suggests that immunity from medical malpractice claims was a driving force behind the legislation[, but] the focus of the immunity analysis was the provision of medical care." *Id*. *3. "[U]nder Section 233(a), '[t]he United States ... in effect insures designated public health officials by standing in their place financially when they are sued for the performance of their medical duties.'" *Id*. (citing *Cuoco v. Moritsugu*, 222 F.3d 99, 108 (2d Cir. 2000)). The court also posited that by providing immunity, "[t]he statute may well enable the Public Health Service to attract better qualified persons to perform medical, surgical and dental functions...." Id.

29. Thus, Defendant is individually liable for data breach claims and may not claim immunity, nor ask for substitution of the United States as a party, here.

V. FACTUAL ALLEGATIONS

DEFENDANT'S BUSINESS

30. Defendant provides behavioral health services to patients located nationally.

31. Throughout this Complaint, all Defendant's associated locations will be referred to collectively as "Defendant."

32. In the ordinary course of receiving health care services from Defendant, each citizen or patient must provide (and Plaintiff did provide) Defendant with sensitive, personal, and private information, such as her:

- address;
- telephone number;
- date of birth;

- Social Security number;
- driver's license number;
- driver's license state;
- medical history;

33. All of Defendant's employees, staff, entities, sites, and locations may share patient information with each other for various purposes, as should be disclosed in a HIPAA compliant privacy notice ("Privacy Policy") that Defendant is required to maintain.

34. Upon information and belief, Defendant's HIPAA Privacy Policy is provided to every patient prior to receiving treatment and upon request.

35. Defendant agreed to and undertook legal duties to maintain the protected health and personal information entrusted to it by Plaintiff and Class Members safely, confidentially, and in compliance with all applicable laws, including the Health Insurance Portability and Accountability Act ("HIPAA").

36. The patient and employee information held by Defendant in its computer system and network included the Private Information of Plaintiff and Class Members.

THE DATA BREACH

37. A Data Breach occurs when cyber criminals intend to access and steal Private Information that has not been adequately secured by a business entity like Defendant.

38. According to the Notice of Data Incident,

> On or about March 18, 2024, Arisa Health experienced a cybersecurity incident that impacted connectivity to our network. Upon learning of this issue, we immediately commenced a prompt and thorough investigation. As part of our investigation, we have been working very closely with external cybersecurity professionals experienced in handling these types of incidents.
>
> After an extensive forensic investigation and manual review, on May 20, 2024 Arisa Health confirmed that between March 1, 2024 and March 18, 2024, certain impacted files containing personal information may have been subject to unauthorized access or acquisition. The potentially impacted information includes full name, address, date of birth, email address, Social

> Security number, medical record number, health insurance number or member ID, certification of substance abuse program completion, medical history and diagnosis, and driver's license number.

39. The HHS requires "[i]f a breach of unsecured protected health information affects *500 or more individuals*, a covered entity must notify the Secretary of the breach without unreasonable delay and in *no case later than 60 calendar days* from the discovery of the breach."[4] Further, if "the number of individuals affected by a breach is uncertain at the time of submission, the covered entity should provide an estimate," and later provide an addendum or correction to HSS.[5]

40. Defendant cannot claim they were unaware of the HHS notification requirements as they complied (at least in part) with those requirements.

41. Plaintiff's notice letter was dated July 19, 2024—around four months after the incident was discovered.

42. Defendant had obligations created by HIPAA, contract, industry standards, common law, and representations made to Class Members, to keep Class Members' Private Information confidential and to protect it from unauthorized access and disclosure.

43. Plaintiff and Class Members provided their Private Information to Defendant with the reasonable expectation and mutual understanding that Defendant would comply with their obligations to keep such information confidential and secure from unauthorized access.

44. Defendant's data security obligations were particularly important given the substantial increase in Data Breaches in the healthcare industry preceding the date of the breach.

---

[4] U.S. Department of Health and Human Services, *Submitting Notice of a Breach to the Secretary* (Feb. 27, 2023) https://www.hhs.gov/hipaa/for-professionals/breach-notification/breach-reporting/index.html (last viewed June 10, 2024) (emphasis added).
[5] *Id.*

45. In 2023, a record 3,205 data breaches occurred, resulting in around 353,027,892 individuals' information being compromised, a 78% increase from 2022.[6] Of the 2023 recorded data breaches, 809 of them, or 25.00%, were in the medical or healthcare industry.[7] The 809 reported breaches reported in 2023 exposed nearly 56 million sensitive records, compared to only 343 breaches that exposed just over 28 million sensitive records in 2022.[8]

46. Data breaches such as the one experienced by Defendant has 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.

47. In fact, according to the cybersecurity firm Mimecast, 90% of healthcare organizations experienced cyberattacks in the past year.[9]

48. Therefore, the increase in such attacks, and attendant risk of future attacks, was widely known to the public and to anyone in Defendant's industry, including Defendant.

DEFENDANT FAILS TO COMPLY WITH FTC GUIDELINES

49. The Federal Trade Commission ("FTC") has promulgated many guides for businesses which show how important it is to implement reasonable data security practices. According to the FTC, the need for data security should shape all business decision-making.

50. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cyber-security guidelines for businesses. The guidelines note that businesses should protect the personal patient information that they keep; properly

---

[6] *See* Identity Theft Resource Center, *2023 Data Breach Report* (January 2024), *available at* https://www.idtheftcenter.org/publication/2023-data-breach-report/ (last visited June 10, 2024).
[7] *Id*.
[8] *Id*. at 11, Fig.3.
[9] Maria Henriquez, *Iowa City Hospital Suffers Phishing Attack, Security Magazine* (Nov. 23, 2020), *available at* https://www.securitymagazine.com/articles/93988-iowa-city-hospital-suffers-phishing-attack (last visited May 21, 2024).

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 any security problems.[10] 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 suggesting 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.[11]

51. The FTC further recommends that companies not maintain PII 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.

52. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect patient 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 also clarify the measures businesses must take to meet their data security obligations.

53. These FTC enforcement actions include actions against healthcare providers 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

[10] Federal Trade Commission, *Protecting Personal Information: A Guide for Business* (2016), *available at* www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited May 21, 2024).
[11] *Id.*

data security practices were unreasonable and constitute an unfair act or practice in violation of Section 5 of the FTC Act.")

54. Defendant failed to properly implement basic data security practices.

55. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to patients' PII and PHI constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

56. Defendant was always fully aware of its obligation to protect the PII and PHI of its patients. Defendant was also aware of the significant repercussions that would result from its failure to do so.

DEFENDANT FAILS TO COMPLY WITH INDUSTRY STANDARDS

57. As shown above, experts studying cyber security routinely identify healthcare providers as being particularly vulnerable to cyberattacks because of the value of the PII and PHI which they collect and maintain.

58. Several best practices have been identified that a minimum should be implemented by healthcare providers like Defendant, including, but not limited to, educating all employees; using strong passwords; creating multi-layer security, including firewalls, antivirus, and anti-malware software; encryption, making data unreadable without a key; using multi-factor authentication; protecting backup data; and limiting which employees can access sensitive data.

59. Other best cybersecurity practices that are standard in the healthcare industry 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; training staff regarding critical points.

60. Defendant failed to meet the minimum standards of any of the following 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.

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

DEFENDANT'S CONDUCT VIOLATES HIPAA AND REVEALS ITS INSUFFICIENT DATA SECURITY

62. HIPAA requires covered entities such as Defendant to protect against reasonably anticipated threats to the security of sensitive patient health information.

63. Covered entities must implement safeguards to ensure the confidentiality, integrity, and availability of PHI. Safeguards must include physical, technical, and administrative components.

64. Title II of HIPAA contains what are known as the Administrative Simplification provisions. 42 U.S.C. §§ 1301, *et seq*. These provisions require, among other things, that the Department of Health and Human Services ("HHS") create rules to streamline the standards for handling PII like the data Defendant left unguarded. The HHS subsequently promulgated multiple regulations under authority of the Administrative Simplification provisions of HIPAA. These rules include 45 C.F.R. § 164.306(a) (1-4); 45 C.F.R. § 164.312(a)(1); 45 C.F.R. § 164.308(a)(1)(i); 45 C.F.R. § 164.308(a)(1)(ii)(D), and 45 C.F.R. § 164.530(b).

65. A Data Breach such as the one Defendant experienced, is considered a breach under the HIPAA Rules because there is an access of PHI not permitted under the HIPAA Privacy Rule:

> A breach under the HIPAA Rules is defined as, "...the acquisition, access, use, or disclosure of PHI in a manner not permitted under the [HIPAA Privacy Rule] which compromises the security or privacy of the PHI." *See* 45 C.F.R. 164.40.

66. Defendant's Data Breach resulted from a combination of insufficiencies that demonstrate they failed to meet mandated by HIPAA regulations.

VI. DEFENDANT'S BREACH

67. Defendant breached its obligations to Plaintiff and Class Members and/or was otherwise negligent and reckless because it failed to properly maintain and safeguard its computer systems and its data. Defendant's unlawful conduct includes, but is not limited to, the following acts and/or omissions:

a. Failing to maintain an adequate data security system to reduce the risk of data breaches and cyber-attacks;

b. Failing to adequately protect patients' Private Information;

c. Failing to properly monitor its own data security systems for existing intrusions;

d. Failing to ensure that vendors with access to Defendant's protected health data employed reasonable security procedures;

e. Failing to ensure the confidentiality and integrity of electronic PHI they created, received, maintained, and/or transmitted, in violation of 45 C.F.R. § 164.306(a)(1);

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

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

h. Failing to implement procedures to review records of information system activity regularly, such as audit logs, access reports, and security incident tracking reports in violation of 45 C.F.R. § 164.308(a)(1)(ii)(D);

i. Failing to protect against reasonably anticipated threats or hazards to the security or integrity of electronic PHI in violation of 45 C.F.R. § 164.306(a)(2);

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

k. Failing to ensure compliance with HIPAA security standard rules by Defendant's workforce in violation of 45 C.F.R. § 164.306(a)(4);

l. Failing to train all members of Defendant's workforce effectively on the policies and procedures about PHI as necessary and appropriate for the members of its workforces to carry out their functions and to maintain security of PHI, in violation of 45 C.F.R. § 164.530(b); and/or

m. Failing to render the electronic PHI they maintained unusable, unreadable, or indecipherable to unauthorized individuals, as they had not encrypted the electronic PHI as specified in the HIPAA Security Rule by "the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key" (45 C.F.R. § 164.304, definition of "encryption").

68. As the result of computer systems needing security upgrading, inadequate procedures for handling emails containing ransomware or other malignant computer code, and inadequately trained employees who opened files containing the ransomware virus, Defendant negligently and unlawfully failed to safeguard Plaintiff's and Class Members' Private Information.

69. Plaintiff and Class Members now face an increased risk of fraud and identity theft.

DATA BREACHES PUT CONSUMERS AT AN INCREASED RISK OF FRAUD AND IDENTIFY THEFT

70. Data Breaches such as the one experienced by Defendant's patients are especially problematic because of the disruption they cause to the overall daily lives of victims affected by the attack.

71. The United States Government Accountability Office released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[12]

72. The FTC recommends that identity theft victims take several steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for 7 years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[13]

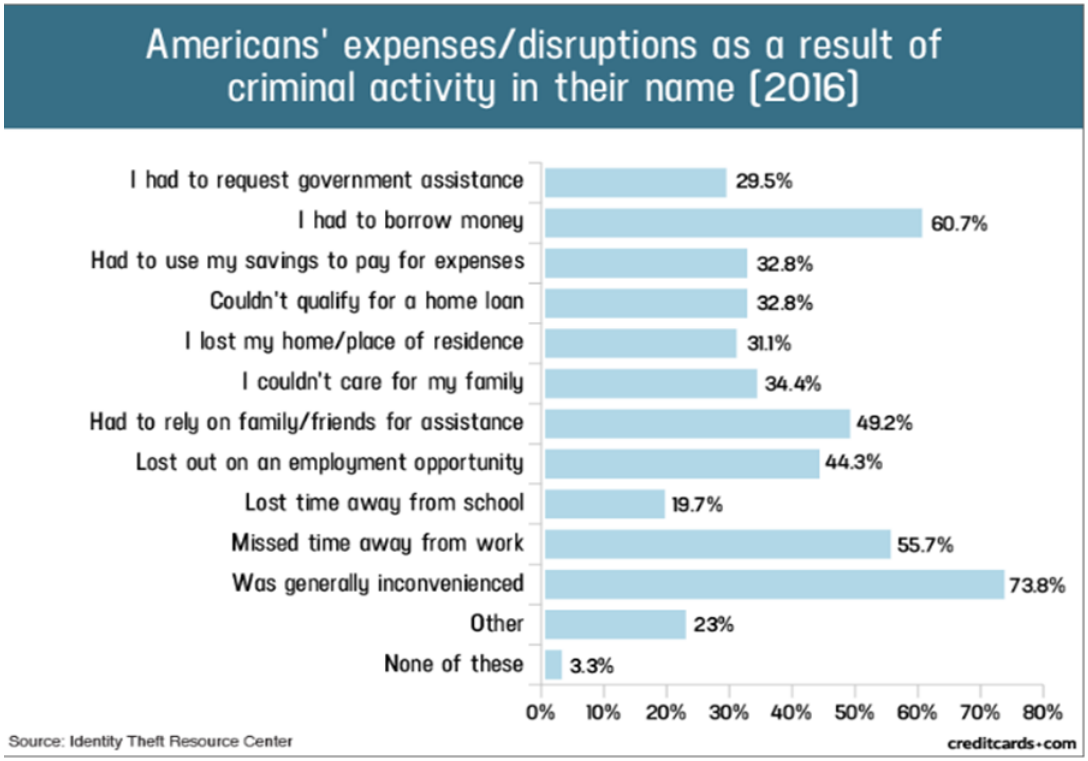
73. Identity thieves use stolen personal information such as Social Security numbers for various crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.

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

[12] U.S. Government Accountability Office, *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown* (June 2007), *available at* https://www.gao.gov/new.items/d07737.pdf (last visited May 21, 2024) ("GAO Report").

[13] Federal Trade Commission, *What To Do Right Away* (2024), *available at* https://www.identitytheft.gov/Steps (last visited June 10, 2024).

75. A study by Identity Theft Resource Center shows the many harms caused by fraudulent use of personal and financial information:[14]



76. Theft of Private Information is also gravely serious. PII/PHI is a valuable property right.[15] Its value is axiomatic, considering the value of Big Data in corporate America and the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that Private Information has considerable market value.

77. Theft of PHI is gravely serious: "A thief may use your name or health insurance numbers to see a doctor, get prescription drugs, file claims with your insurance provider, or get other care. If the thief's health information is mixed with yours, your treatment, insurance and

[14] Jason Steele, *Credit Card and ID Theft Statistics* (Oct. 24, 2017), *available at* https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276.php (last visited March 10, 2022).

[15] *See, e.g.,* John T. Soma, et al, *Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets*, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

payment records, and credit report may be affected."[16] Drug manufacturers, medical device manufacturers, pharmacies, hospitals and other healthcare service providers often purchase PII/PHI on the black market for the purpose of target marketing their products and services to the physical maladies of the data breach victims themselves. Insurance companies purchase and use wrongfully disclosed PHI to adjust their insureds' medical insurance premiums.

78. It must also be noted there may be a substantial time lag—measured in years—between when harm occurs versus when it is discovered, and between when Private Information and/or financial information is stolen and when it is used. According to the U.S. Government Accountability Office, which studied data breaches:

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

See GAO Report, at p. 29.

79. Private Information and financial information are such valuable commodities to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black-market" for years.

80. There is a strong probability that all the stolen information has been dumped on the black market or will be dumped on the black market, meaning Plaintiff and Class Members are at an increased risk of fraud and identity theft for many years into the future. Thus, Plaintiff and Class Members must vigilantly monitor their financial and medical accounts for many years to come.

[16] *See* Federal Trade Commission, *Medical Identity Theft*, *available at* http://www.consumer.ftc.gov/articles/0171-medical-identity-theft (last visited May 21, 2024).

81. Sensitive Private Information can sell for as much as $363 per record according to the Infosec Institute.[17] PII is particularly valuable because criminals can use it to target victims with frauds and scams. Once PII is stolen, fraudulent use of that information and damage to victims may continue for years.

82. For example, the Social Security Administration has warned that identity thieves can use an individual's Social Security number to apply for more credit lines.[18] Such fraud may go undetected until debt collection calls commence months, or even years, later. Stolen Social Security Numbers also make it possible for thieves to file fraudulent tax returns, file for unemployment benefits, or apply for a job using a false identity.[19] Each of these fraudulent activities is difficult to detect. An individual may not know that his or his Social Security Number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

83. It is also hard to change or cancel a stolen Social Security number.

84. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. Even then, a new Social Security number may not be effective, as "[t]he credit bureaus and banks are able to link the new number very quickly to the

[17] Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, InfoSec (July 27, 2015), *available at* https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/ (last visited May 21, 2024).
[18] Social Security Administration, *Identity Theft and Your Social Security Number* (2018), *available at* https://www.ssa.gov/pubs/EN-05-10064.pdf (last visited May 21, 2024).
[19] *Id* at 4.

old number, so all of that old bad information is quickly inherited into the new Social Security number."[20]

85. This data, as one would expect, demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "[c]ompared to credit card information, personally identifiable information and Social Security Numbers are worth more than 10x on the black market."[21]

86. Medical information is especially valuable to identity thieves. According to account monitoring company LogDog, coveted Social Security numbers were selling on the dark web for just $1 in 2016—the same as a Facebook account. That pales in comparison with the asking price for medical data, which was selling for $300 and up.[22]

87. In recent years, the medical and financial services industries have experienced disproportionally higher numbers of data theft events than other industries. Defendant therefore knew or should have known this and strengthened their data systems accordingly. Defendant were put on notice of the substantial and foreseeable risk of harm from a data breach, yet they failed to properly prepare for that risk.

VII. PLAINTIFF'S EXPERIENCES

88. Plaintiff Nicholas Burgess is and at all times mentioned herein was an individual citizen residing in the State of Arkansas, in the city of Mayflower.

---

[20] Brian Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (February 9, 2015), *available at* http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft (last visited May 21, 20240.

[21] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, Computer World (Feb. 6, 2015), *available at* http://www.itworld.com/article/2880960/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last visited March 10, 2022).

[22] Paul Ducklin, *FBI "ransomware warning" for healthcare is a warning for everyone!*, Sophos (Oct. 29, 2020) *available at* https://news.sophos.com/en-us/2020/10/29/fbi-ransomware-warning-for-healthcare-is-a-warning-for-everyone/ (last visited March 10, 2022).

89. Plaintiff used Defendant's services, requiring him to provide his Private Information to Defendant.

90. After Plaintiff provided Private Information, Defendant suffered a Data Breach.

91. Plaintiff used Defendant's services before the Data Breach.

92. When Plaintiff received his Notice Letter, sent July 19, the letter stated that his PII and PHI may have been either accessed and/or acquired by an unauthorized individual including Plaintiff's "Address, date of birth, email address, Social Security number, medical record number, health insurance number, medical history and diagnosis, and driver's license number." Exhibit A.

93. Plaintiff is especially alarmed by the amount of stolen or accessed PII and PHI listed on his letter. Despite Defendant providing that list, he cannot be sure more of his PII or PHI was exfiltrated. Now he checks his bank accounts and credit cards throughout the day each day, spending approximately an hour per week just monitoring accounts because of Defendant's Data Breach.

94. Plaintiff knows that cybercriminals often sell Private Information, and that his PII or PHI could be abused months or even years after a data breach.

95. Had Plaintiff been aware that Defendant's computer systems were not secure, he would not have entrusted Defendant with his personal data.

VIII. PLAINTIFF'S AND CLASS MEMBERS' DAMAGES

96. To date, Defendant has done absolutely nothing to compensate Plaintiff and Class Members for the damages they sustained in the Data Breach.

97. Defendant's failure to compensate is wholly inadequate as it fails to sufficiently compensate all victims of the Data Breach, who commonly face multiple years of ongoing identity theft, and it entirely provides no compensation for its unauthorized release and disclosure of Plaintiff's and Class Members' Private Information.

98. Furthermore, Defendant's credit monitoring advice to Plaintiff and Class Members places the burden on Plaintiff and Class Members, rather than on Defendant, to investigate and protect themselves from Defendant's tortious acts resulting in the Data Breach. Rather than automatically enrolling Plaintiff and Class Members in credit monitoring services upon discovery of the breach, Defendant merely sent instructions to Plaintiff and Class Members about actions they can affirmatively take to protect themselves.

99. Plaintiff and Class Members have been damaged by the compromise and exfiltration of their Private Information in the Data Breach, and by the severe disruption to their lives as a direct and foreseeable consequence of this Data Breach.

100. Plaintiff's Private Information was compromised and exfiltrated by cyber-criminals as a direct and proximate result of the Data Breach.

101. Plaintiff was damaged in that his Private Information is in the hands of cyber criminals.

102. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have been placed at an actual, present, immediate, and continuing increased risk of harm from fraud and identity theft.

103. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have been forced to expend time dealing with the effects of the Data Breach.

104. Plaintiff and Class Members face substantial risk of out-of-pocket fraud losses such as loans opened in their names, medical services billed in their names, tax return fraud, utility bills opened in their names, credit card fraud, and similar identity theft.

105. Plaintiff and Class Members face substantial risk of being targeted for future phishing, data intrusion, and other illegal schemes based on their Private Information as potential

fraudsters could use that information to more effectively target such schemes to Plaintiff and Class Members.

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

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

108. Plaintiff and Class Members have spent and will continue to spend significant amounts of time to monitor their financial accounts and records for misuse.

109. Plaintiff and Class Members have suffered or will suffer actual injury as a direct result of the Data Breach. Many victims suffered ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach relating to:

a. Finding fraudulent charges;

b. Canceling and reissuing credit and debit cards;

c. Purchasing credit monitoring and identity theft prevention;

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

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

f. Placing “freezes” and “alerts” with credit reporting agencies;

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

h. Contacting financial institutions and closing or modifying financial accounts;

i. Resetting automatic billing and payment instructions from compromised credit and debit cards to new ones;

j. Paying late fees and declined payment fees imposed because of failed automatic payments that were tied to compromised cards that had to be cancelled; and

k. Closely reviewing and monitoring bank accounts and credit reports for unauthorized activity for years to come.

110. Moreover, Plaintiff and Class Members have an interest in ensuring that their Private Information, which is believed to remain in the possession of Defendant, is protected from further breaches by implementing security measures and safeguards, including, but not limited to, making sure that the storage of data or documents containing personal and financial information is inaccessible online and that access to such data is password-protected.

111. Further, because of Defendant's conduct, Plaintiff and Class Members are forced to live with the anxiety that their Private Information —which contains the most intimate details about a person's life—may be disclosed to the entire world, thereby subjecting them to embarrassment and depriving them of any right to privacy whatsoever.

112. As a direct and proximate result of Defendant's actions and inactions, Plaintiff and Class Members have suffered anxiety, emotional distress, and loss of privacy, and are at an increased risk of future harm.

IX. CLASS ACTION ALLEGATIONS

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

114. Plaintiff proposes the following Class definition, subject to amendment as appropriate:

All persons whose Private Information was compromised because of the March 1-18, 2024 Data Breach (the "Class").

115. Excluded from the Class are Defendant's 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.

116. Plaintiff reserves the right to amend or modify the class definitions with greater specificity or division after having an opportunity to conduct discovery. The proposed Class meets the criteria for certification under Rule 23.

117. Numerosity. The Members of the Class are so numerous that joinder of all of them is impracticable. The exact number of Class Members is unknown to Plaintiff now, but Defendant has provided notice to Texas's Attorney General that the number is at least 1,434 Texans.

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

a. Whether Defendant unlawfully used, maintained, lost, or disclosed Plaintiff's and Class Members' Private Information;

b. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information 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 adhered to industry standards;

e. Whether Defendant owed a duty to Class Members to safeguard their Private Information;

f. Whether Defendant breached its duty to Class Members to safeguard their Private Information;

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

h. Whether Plaintiff and Class Members suffered legally cognizable damages from Defendant's misconduct;

i. Whether Defendant's conduct was negligent;

j. Whether Defendant's conduct was per se negligent;

k. Whether Defendant's acts, inactions, and practices complained of herein amount to acts of intrusion upon seclusion under the law;

l. Whether Defendant were unjustly enriched;

m. Whether Defendant failed to provide notice of the Data Breach promptly; and

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

119. Typicality. Plaintiff's claims are typical of those of other Class Members because Plaintiff's Private Information, like that of every other Class member, was compromised in the Data Breach. Plaintiff's claims are typical of those of the other Class Members because, among other things, all Class Members were injured through the common misconduct of Defendant. Plaintiff are advancing the same claims and legal theories on behalf of themselves and all other Class Members, and no defenses are unique to Plaintiff. Plaintiff's claims and those of Class Members arise from the same operative facts and are based on the same legal theories.

120. 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, including data privacy litigation of this kind.

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

122. 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.

123. 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.

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

125. Likewise, issues under Rule 23 are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance matter and the parties' interests therein. Such issues include, but are not limited to:

a. Whether Defendant failed to timely notify the public of the Data Breach;

b. Whether Defendant owed a legal duty to Plaintiff and the Class to exercise due care in collecting, storing, and safeguarding their Private Information;

c. Whether Defendant's security measures to protect their data systems were reasonable considering best practices recommended by data security experts;

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

e. Whether Defendant failed to take commercially reasonable steps to safeguard consumer Private Information; and

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

126. 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.

X. CAUSES OF ACTION

FIRST COUNT
NEGLIGENCE
(On Behalf of Plaintiff and All Class Members)

127. Plaintiff re-alleges and incorporates the above allegations as if fully set forth herein.

128. Defendant required Plaintiff and Class Members to submit non-public personal information to obtain healthcare/dental services and/or employment.

129. By collecting and storing this data in Defendant's computer property, 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' Private Information held within it—to prevent disclosure of the information, and to safeguard the information from theft. Defendant's duty included a responsibility to implement processes by which it could detect a breach of its security systems in a reasonably expeditious period and to give prompt notice to those affected in the case of a Data Breach.

130. 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 Private Information.

131. Defendant's duty of care to use reasonable security measures arose because of the special relationship that existed between Defendant and its patients, which is recognized by laws

and regulations including, but not limited to, HIPAA, as well as common law. Defendant could ensure that its systems were sufficient to protect against the foreseeable risk of harm to Class Members from a Data Breach or data breach.

132. 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)(1). Some or all the healthcare, dental, and/or medical information at issue constitutes "protected health information" within the meaning of HIPAA.

133. In addition, 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.

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

135. Defendant breached its duties, and thus were negligent, by failing to use reasonable measures to protect Class Members' Private Information. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

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

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

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

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

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

f. Failing to timely notify Class Members about the Data Breach so that they could take appropriate steps to mitigate the potential for identity theft and other damages; and

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

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

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

138. Plaintiff and Class Members are entitled to compensatory and consequential damages suffered because of the Data Breach.

139. Defendant's negligent conduct is ongoing, in that they still hold the Private Information of Plaintiff and Class Members in an unsafe and unsecure manner.

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

SECOND COUNT
BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiff and All Class Members)

141. Plaintiff re-alleges and incorporates the above allegations as if fully set forth herein.

142. When Plaintiff and Class Members provided their Private Information to Defendant in exchange for Defendant's services and/or employment, they entered implied contracts with Defendant under which Defendant agreed to reasonably protect such information.

143. Defendant solicited, offered, and invited Class Members to provide their Private Information as part of Defendant's regular business practices. Plaintiff and Class Members accepted Defendant's offers and provided their Private Information to Defendant.

144. In entering such implied contracts, Plaintiff and Class Members reasonably believed and expected that Defendant's data security practices complied with relevant laws and regulations, including HIPAA, and adhered to industry standards.

145. Plaintiff and Class Members paid money to Defendant or provided labor 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.

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

147. Plaintiff and Class Members would not have entrusted their Private Information to Defendant in the absence of its implied promise to monitor its computer systems and networks to ensure that they adopted reasonable data security measures.

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

149. Defendant breached its implied contracts with Class Members by failing to safeguard and protect their Private Information.

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

151. Plaintiff and Class Members are entitled to compensatory, consequential, and nominal damages suffered because of the Data Breach.

152. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to, e.g., (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit monitoring to all Class Members.

THIRD COUNT
NEGLIGENCE *PER SE*
(On Behalf of Plaintiff and All Class Members)

153. Plaintiff re-alleges and incorporates the above allegations as if fully set forth herein.

154. Under the Federal Trade Commission Act, 15 U.S.C. § 45, Defendant had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' Private Information.

155. Under HIPAA, 42 U.S.C. § 1302d, et seq., Defendant had a duty to implement reasonable safeguards to protect Plaintiff's and Class Members' Private Information.

156. Under HIPAA, Defendant had a duty to render the electronic PHI they maintained unusable, unreadable, or indecipherable to unauthorized individuals, as specified in the HIPAA Security Rule by "the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key." See definition of encryption at 45 C.F.R. § 164.304.

157. Defendant breached its duties to Plaintiff and Class Members under the Federal Trade Commission Act and HIPAA by failing to provide fair, reasonable, or adequate computer

systems and data security practices to safeguard Plaintiff's and Class Members' Private Information.

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

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

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

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

FOURTH COUNT
BREACH OF FIDUCIARY DUTY
(On Behalf of Plaintiff and All Class Members)

162. Plaintiff re-alleges and incorporates the above allegations as if fully set forth herein.

163. Defendant became guardian of Plaintiff's and Class Members' Private Information, creating a special relationship between Defendant and Plaintiff and Class Members.

164. As such, Defendant became a fiduciary by its undertaking and guardianship of the Private Information, to act primarily for Plaintiff and Class Members, (1) for the safeguarding of Plaintiff's and Class Members' Private Information; (2) to timely notify Plaintiff and Class Members of a Data Breach and disclosure; and (3) to maintain complete and accurate records of what information (and where) Defendant did and does store.

165. Defendant has a fiduciary duty to act for the benefit of Plaintiff and Class Members upon matters within the scope of Defendant's relationship with its patients, in particular, to keep secure their Private Information.

166. Defendant breached its fiduciary duties to Plaintiff and Class Members by failing to encrypt and otherwise protect the integrity of the systems containing Plaintiff's and Class Members' Private Information.

167. Defendant breached its fiduciary duties owed to Plaintiff and Class Members by failing to timely notify and/or warn Plaintiff and Class Members of the Data Breach.

168. Defendant breached its fiduciary duties to Plaintiff and Class Members by otherwise failing to safeguard Plaintiff's and Class Members' Private Information.

169. As a direct and proximate result of Defendant's breaches of its fiduciary duties, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to:

a. actual identity theft;

b. the compromise, publication, and/or theft of their Private Information;

c. out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their Private Information;

d. lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest, and recover from identity theft;

e. the continued risk to their Private Information, 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 the Private Information in its continued possession;

f. future costs in terms of time, effort, and money that will be expended as result of the Data Breach for the rest of the lives of Plaintiff and Class Members; and

g. the diminished value of Defendant's services they received.

170. As a direct and proximate result of Defendant's breach of its fiduciary duties, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm, and other economic and non-economic losses.

FIFTH COUNT
UNJUST ENRICHMENT
(On Behalf of Plaintiff and All Class Members)

171. Plaintiff re-alleges and incorporates the above allegations as if fully set forth herein.

172. Plaintiff brings this claim individually and on behalf of all Class Members. This count is plead in the alternative to the breach of contract count above.

173. Upon information and belief, Defendant fund its data security measures entirely from its general revenue, including payments made by or on behalf of Plaintiff and the Class Members.

174. As such, a portion of the payments made by or on behalf of Plaintiff and the 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.

175. Plaintiff and Class Members conferred a monetary benefit on Defendant. They bought goods and services from Defendant and/or its agents and in so doing provided Defendant with their Private Information. In exchange, Plaintiff and Class Members should have received from Defendant the goods and services that were the subject of the transaction and have their Private Information protected with adequate data security.

176. Defendant knew that Plaintiff and Class Members conferred a benefit which Defendant accepted. Defendant profited from these transactions and used the Private Information of Plaintiff and Class Members for business purposes.

177. Defendant enriched themselves by saving the costs Defendant reasonably should have expended on data security measures to secure Plaintiff's and Class Members' Personal

Information. Rather than providing a reasonable level of security that would have prevented the hacking incident, Defendant instead calculated to increase its own profits at the expense of Plaintiff and Class Members by using cheaper, ineffective security measures. 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.

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

179. Defendant failed to secure Plaintiff's and Class Members' Private Information and thus did not provide full compensation for the benefit Plaintiff and Class Members provided.

180. Defendant acquired the Private Information through inequitable means in that they failed to disclose the inadequate security practices alleged.

181. If Plaintiff and Class Members knew that Defendant had not reasonably secured their Private Information, they would not have agreed to provide their Private Information to Defendant.

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

183. 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:

a. actual identity theft;

b. the loss of the opportunity of how their Private Information is used;

c. the compromise, publication, and/or theft of their Private Information;

d. out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their Private Information;

e. lost opportunity costs associated with efforts expended and the loss of productivity addressing and attempting to mitigate the consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest, and recover from identity theft;

f. the continued risk to their Private Information, 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 Private Information in its continued possession; and

g. future costs in terms of time, effort, and money to be expended to prevent, detect, contest, and repair the effect of the Private Information compromised because of the Data Breach for the rest of the lives of Plaintiff and Class Members.

184. 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.

185. 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 services.

SIXTH COUNT
DECLARATORY JUDGMENT
(On Behalf of Plaintiff and All Class Members)

186. Plaintiff re-alleges and incorporates the above allegations as if fully set forth herein.

187. Under the Declaratory Judgment Act, 28 U.S.C. § 2201, et seq., this Court may enter a judgment declaring the rights and legal relations of the parties and to grant further necessary relief. Furthermore, the Court has broad authority to restrain acts that are tortious and violate the terms of the federal laws and regulations and state statute[s] described in this Complaint.

188. Defendant owes a duty of care to Plaintiff and Class Members, which required them to adequately secure Plaintiff's and Class Members' Private Information.

189. Defendant still possess Private Information about Plaintiff and Class Members.

190. Plaintiff alleges that Defendant's data security measures remain inadequate. Furthermore, Plaintiff continue to suffer injury because of the compromise of their Private Information and the risk remains that further compromises of their Private Information will recur.

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

a. Defendant owes a legal duty to secure its patients' Private Information and to timely notify them of a data breach under the common law, HIPAA, and the FTCA;

b. Defendant's existing security measures do not comply with its explicit or implicit contractual obligations and duties of care to provide reasonable security procedures and practices that are appropriate to protect their patients' Private Information; and

c. Defendant continues to breach this legal duty by failing to employ reasonable measures to secure its patients' Private Information.

192. This Court should also issue corresponding prospective injunctive relief requiring Defendant to employ adequate security protocols consistent with legal and industry standards to protect its patients' Private Information, including the following.

a. Order Defendant to provide lifetime credit monitoring and identity theft insurance to Plaintiff and Class Members.

b. Order that, to comply with Defendant's explicit or implicit contractual obligations and duties of care, Defendant must implement and maintain reasonable security measures, including, but not limited to:

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

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

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

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

v. conducting regular database scanning and security checks;

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

vii. meaningfully educating its clients and patients about the threats faced regarding the security of their Private Information.

193. If an injunction is not issued, Plaintiff will suffer irreparable injury and will lack an adequate legal remedy to prevent another data breach at Defendant. The risk of another such breach is real, immediate, and substantial. If another breach at Defendant occurs, Plaintiff will not have an adequate remedy at law because many of the resulting injuries are not readily quantifiable.

194. The hardship to Plaintiff if an injunction does not issue exceeds the hardship to Defendant if an injunction is issued. Plaintiff will likely be subjected to substantial, continued identity theft and related damages if an injunction is not issued. On the other hand, the cost of Defendant's compliance with an injunction requiring reasonable prospective data security measures is minimal, and Defendant has a preexisting legal obligation to employ such measures.

195. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing a subsequent data breach at Defendant, thus preventing future injury to Plaintiff, other patients, and other employees whose Private Information would be further compromised.

XI. PRAYER FOR RELIEF

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

a. For an Order certifying this action as a class action under Federal Rule of Civil Procedure, defining the Class as requested herein, appointing Plaintiff and their counsel to represent the Class, and finding that Plaintiff are proper representatives of the Class requested herein;

b. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein relating to the misuse and/or disclosure of Plaintiff's and Class Members' Private Information, and from refusing to issue prompt, complete and accurate disclosures to Plaintiff and Class Members;

c. For equitable relief compelling Defendant to use appropriate methods and policies related to consumer data collection, storage, and safety, and to disclose with specificity the type of Private Information compromised during the Data Breach;

d. For equitable relief requiring restitution and disgorgement of the revenues wrongfully retained because of Defendant's wrongful conduct;

e. Ordering Defendant to pay for not less than ten years of credit monitoring services for Plaintiff and the Class;

f. For an award of actual damages, compensatory damages, statutory damages, and statutory penalties, in an amount to be determined, as allowable by law;

g. For an award of punitive damages, as allowable by law;

h. For an award of attorneys' fees and costs, and any other expense, including expert witness fees;

i. Pre- and post-judgment interest on any amounts awarded; and

j. Any other relief that this court may deem just and proper.

XII. JURY TRIAL DEMANDED

Plaintiff still demand a trial by jury on all claims so triable.

Dated: July 30, 2024

Respectfully submitted,

/s/ Martha Tucker Ayres

Martha Tucker Ayres
Arkansas Bar No. AR2012233
TABLE LAW PLLC
Markham Executive Center
10201 W. Markham St., Suite 311
Little Rock, AR 72205
Phone: 501-491-0300

EKSM, LLP
Leigh S. Montgomery*
Texas Bar No. 24052214
leigh@ellzeylaw.com
1105 Milford Street
Houston, Texas 77006
Phone: (888) 350-3931
Fax: (888) 276-3455

ATTORNEYS FOR PLAINTIFF
(* denotes *pro hac vice* forthcoming)

Exhibit A

Arisa Health Inc.
c/o Cyberscout
PO Box 1286
Dearborn, MI 48120-9998

PKCIAH00Z01724
NICHOLAS LYNN BURGESS
495 HWY 365 APT 5
MAYFLOWER, AR 72106-8803

arisa health

July 19, 2024

Important Information Please Review Carefully

Dear NICHOLAS BURGESS:

The privacy and security of the personal information we maintain is of the utmost importance to Arisa Health Incorporated ("Arisa Health"). Please note, Arisa Health has multiple subsidiaries, including Counseling Associates, Inc., Northeast Arkansas Community Mental Health Center d/b/a Mid-South Health Systems, Ozark Guidance Center, Inc., and Professional Counseling Associates. Inc. We were provided some of your personal information through services you received from Arisa and / or one of our subsidiaries. We are writing with important information regarding a data security incident. As such, we want to provide you with information about the incident, tell you about the services that we are providing to you, and let you know that we continue to take significant measures to protect your information.

What Happened?

On or about March 18, 2024, Arisa Health experienced a cybersecurity incident that impacted connectivity to our network.

What We Are Doing

Upon learning of this issue, we immediately commenced a prompt and thorough investigation. As part of our investigation, we have been working very closely with external cybersecurity professionals experienced in handling these types of incidents. After an extensive forensic investigation and comprehensive document review, on May 20, 2024, we determined your personal data may have been subject to unauthorized access or acquisition, which occurred between March 1, 2024 and March 18, 2024.

What Information Was Involved?

The information potentially impacted includes your Address, date of birth, email address, Social Security number, medical record number, Health plan beneficiary number, driver's license number and medical history & diagnosis.

What You Can Do

We have no evidence that any of your information has been misused. To protect you from potential misuse of your information, we are offering a complimentary twelve (12)-month membership of Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score services at no charge. This notification is sent to you the same day that the change or update takes place with the bureau. Finally, we are providing you with proactive fraud assistance to help with any questions that you might have or in the event that you become a victim of fraud. These services will be provided by Cyberscout, a TransUnion company specializing in fraud assistance and remediation services.

PKCIAH00Z01724017240103030400