

FILED
U.S. DISTRICT COURT
EASTERN DISTRICT ARKANSAS

MAY 16 2022

TAMMY H. DOWNS, CLERK
By: *[Signature]*
DEP. CLERK

UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF ARKANSAS
CENTRAL DIVISION

JESSICA WHITE,
on behalf of herself and all others similarly
situated,

Plaintiff,

vs.

ARCARE,

Registered Agent:
CT Corporation System
124 West Capitol Avenue, Suite 1900,
Little Rock, Arkansas, 72201

Defendant.

NO. *4:22CV454-KGB*

CLASS ACTION COMPLAINT

JURY DEMAND

This case assigned to District Judge *Baker*
and to Magistrate Judge *Harris*

Plaintiff Jessica White (“Plaintiff”), individually and on behalf of all others similarly situated (“Class Members”), brings this Class Action Complaint against Arcare (“Arcare” or “Defendant”), and alleges, upon personal knowledge as to her own actions and her counsels’ investigations, and upon information and belief as to all other matters, as follows:

I. INTRODUCTION

1. Plaintiff brings this class action against Defendant for its failure to properly secure and safeguard personally identifiable information and protected health information (“PHI”) that Defendant’s patients entrusted to it, including, without limitation, names, Social Security numbers, driver’s license or state identification numbers, dates of birth, financial account information, medical treatment information, prescription information, medical diagnosis or condition information, and health insurance information (collectively, “personally identifiable information”

or “PII”).¹

2. ARcare is a health care system with over seventy-four facilities across Arkansas, Mississippi, and Kentucky.² ARcare employed over 149 providers.³ According to public records, Defendant’s revenue for the fiscal year ending in 2019 totaled \$90,136,910.⁴

3. According to Defendant, ARcare “treats its responsibility to safeguard information in its care as an utmost priority.”⁵

4. On or about March 14, 2022, ARcare determined that “an unauthorized actor may have accessed and/or acquired some sensitive data during a period of unauthorized access to ARcares computer systems between January 18, 2022, and February 24, 2022” (the “Data Breach”).⁶

5. During the Data Breach, the attacker actually or potentially compromised the personal information of more than 345,353 current or former patients of Defendant.⁷

6. On or around April 25, 2022, Defendant began notifying state and federal regulators of the Data Breach.

7. On or around April 25, 2022, Defendant began notifying Plaintiff and Class Members of the Data Breach.

8. By obtaining, collecting, using, and deriving a benefit from Plaintiff’s and Class Members’ PII and PHI, Defendant assumed legal and equitable duties to those individuals.

¹ Personally identifiable information generally incorporates information that can be used to distinguish or trace an individual’s identity, either alone or when combined with other personal or identifying information. 2 CFR § 200.79. At a minimum, it includes all information that on its face expressly identifies an individual. PII also is generally defined to include certain identifiers that do not on their face name an individual, but that are considered to be particularly sensitive and/or valuable if in the wrong hands (for example, Social Security number, passport number, driver’s license number, financial account number).

² <https://www.arcare.net/locations/> (last visited May 10, 2022).

³ <https://www.arcare.net/our-providers/> (last visited May 10, 2022).

⁴ See <https://projects.propublica.org/nonprofits/organizations/581666179> (last visited May 10, 2022).

⁵ Exhibit 1 (“Website Notice”).

⁶ *Id.*

⁷ U.S. DEP’T OF HEALTH & HUMAN SERV., *Breach Portal*, https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf. (last visited May 10, 2022).

9. The exposed PII and PHI of Plaintiff and Class Members can be sold on the dark web. Hackers can access and then offer for sale the unencrypted, unredacted PII and PHI to criminals. Plaintiff and Class Members face a lifetime risk of identity theft, which is heightened here by the loss of Social Security numbers. Plaintiff has already experienced and will continue to experience various instances of fraud, as detailed herein, for years to come.

10. This PII and PHI was actually or potentially compromised due to Defendant's negligent and/or careless acts and omissions and the failure to protect the PII and PHI of Plaintiff and Class Members.

11. Plaintiff brings this action on behalf of all persons whose PII and PHI was actually or potentially compromised as a result of Defendant's failure to: (i) adequately protect the PII and PHI of Plaintiff and Class Members; (ii) warn Plaintiff and Class Members of its inadequate information security practices; and (iii) avoid sharing the PII and PHI of Plaintiff and Class Members without adequate safeguards. Defendant's conduct amounts to negligence and violates federal and state statutes.

12. Plaintiff and Class Members have suffered injury as a result of Defendant's conduct. These injuries include: (i) lost or diminished value of PII and PHI; (ii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII and PHI; (iii) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time, and significantly (iv) the continued and certainly an increased risk to their PII and PHI, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) may remain backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII and PHI.

13. Defendant disregarded the rights of Plaintiff and Class Members by intentionally,

willfully, recklessly, or negligently failing to take and implement adequate and reasonable measures to ensure that Plaintiff's and Class Members' PII and PHI was safeguarded, failing to take available steps to prevent an unauthorized disclosure of data, and failing to follow applicable, required and appropriate protocols, policies and procedures regarding the encryption of data, even for internal use. As the result, the PII and PHI of Plaintiff and Class Members was actually or potentially compromised through disclosure to and/or acquisition by an unknown and unauthorized third party. Plaintiff and Class Members have a continuing interest in ensuring that their information is and remains safe, and they should be entitled to injunctive and other equitable relief.

II. PARTIES

14. Plaintiff Jessica White is a citizen of Arkansas, residing in Pulaski County, Arkansas.

15. Defendant ARcare is an Arkansas corporation organized under the laws of Arkansas and headquartered in Augusta, Arkansas, with its principal place of business in Augusta, Arkansas. Defendant's principal place of business is 117 S 2nd St; Augusta, AR 72006.⁸

16. The true names and capacities of persons or entities, whether individual, corporate, associate, or otherwise, who may be responsible for some of the claims alleged herein are currently unknown to Plaintiff. Plaintiff will seek leave of court to amend this complaint to reflect the true names and capacities of such other responsible parties when their identities become known.

17. All of Plaintiff's claims stated herein are asserted against Defendant and any of its owners, predecessors, successors, subsidiaries, agents and/or assigns.

⁸https://www.sos.arkansas.gov/corps/search_corps.php?DETAIL=56108&corp_type_id=&corp_name=ARcare&agent_search=&agent_city=&agent_state=&filing_number=&cmd= (last visited May 10, 2022).

III. JURISDICTION AND VENUE

18. This Court has subject matter and diversity jurisdiction over this action under 28 U.S.C. § 1332(d) because this is a class action wherein the amount of controversy exceeds the sum or value of \$5 million, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one Class Member is a citizen of a state different from Defendant to establish minimal diversity.

19. The Eastern District of Arkansas has personal jurisdiction over Defendant named in this action because Defendant and/or its parents or affiliates are headquartered in this District and Defendant conduct substantial business in Arkansas and this District through its headquarters, offices, parents, and affiliates.

20. Venue is proper in this District under 28 U.S.C. §1391(b) because Defendant and/or its parents or affiliates are headquartered in this District and a substantial part of the events or omissions giving rise to Plaintiff's claims occurred in this District.

IV. FACTUAL ALLEGATIONS

Background

21. Defendant ARcare is a nonprofit medical system that offers medical services “across Arkansas, Kentucky, and Mississippi for every member of your family.”⁹ ARcare states that it is “committed to you and your health, and we aim to provide the most effective, compassionate care possible to reflect this commitment daily.”¹⁰

22. Prior to the Data Breach, Defendant posted on its website a document entitled “ARcare’s Privacy Statement” (“Privacy Policy”) which describes for patients and clients “how health information about you (as a patient of this practice) may be used and disclosed, and how

⁹ <https://www.arcare.net/> (last visited May 10, 2022).

¹⁰ *Id.*

you can get access to your individually identifiable health information. Please review this notice carefully.”¹¹

23. The Privacy Policy states that Defendant’s “practice is dedicated to maintaining the privacy of your individually identifiable health information as protected by law, including the Health Information Portability and Accountability Act (HIPAA).”¹²

24. The Privacy Policy lists numerous circumstances under which a patient’s PII could be disclosed without their prior written consent, none of which are at issue here. Under “Uses and Disclosures of Your PII in Certain Special Circumstances,” the Privacy Policy provides “categories [that] describe unique scenarios in which we may use or disclose your personally identifiable health information,” none of these are applicable to the Data Breach at issue here.¹³

25. Defendant also provides patients with a “Patient Rights and Responsibilities” document (“Patient Rights”).¹⁴ Under “Confidentiality,” it states

The patient had the right to every consideration of privacy concerning medical records. All records and communications pertaining to medical care will be confidential. Those not directly involved in the patient care must have the permission of the patient to be present.¹⁵

26. Defendant collected and stored some of Plaintiff’s and Class Members’ most sensitive and confidential personal and medical information, including, without limitation names, Social Security numbers, driver’s license or state identification numbers, dates of birth, financial account information, medical treatment information, prescription information, medical diagnosis or condition information, and health insurance information.¹⁶ This includes information that is static, does not change, and can be used to commit myriad financial crimes.

¹¹ ARCARE, Privacy Statement, *available at* <https://www.arcare.net/privacy-statement/> (last visited May 10, 2022).

¹² *Id.*

¹³ *Id.*

¹⁴ Exhibit 2 (“Patient Rights and Responsibilities”).

¹⁵ *Id.*

¹⁶ Ex. 1.

27. ARcare states that it is “committed to you and your health, and we aim to provide the most effective, compassionate care possible to reflect this commitment daily.”¹⁷

28. As a condition of obtaining healthcare services from Defendant, Plaintiff and Class Members were required to provide their PII and PHI to Defendant.

29. Plaintiff and Class Members relied on this sophisticated Defendant to keep their PII and PHI confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information. Plaintiff and Class Members demand security to safeguard their PII and PHI.

30. Defendant had a duty to adopt reasonable measures to protect Plaintiff’s and Class Members’ PII and PHI from involuntary disclosure to third-parties.

The Data Breach

31. Defendant has a posted “Notice of Data Security Incident” on its website (“Website Notice”).¹⁸ The Website Notice reads, in part, as follows:

ARcare is notifying certain individuals of a recent data privacy incident that may impact the privacy of a limited amount of personal and/or medical information. ARcare is unaware of any misuse of individual information and is providing notice to potentially affected individuals out of an abundance of caution.

About the Incident

On February 24, 2022, ARcare experienced a data security incident that impacted its computer systems and caused a temporary disruption to services. ARcare immediately worked to secure its systems and quickly commenced an investigation to confirm the nature and scope of the incident. On March 14, 2022, the investigation determined that an unauthorized actor may have accessed and/or acquired some sensitive data during a period of unauthorized access to ARcares computer systems between January 18, 2022 and February 24, 2022. A thorough review of the contents of the affected data was subsequently performed to determine whether it contained any sensitive information and identify affected

¹⁷ <https://www.arcare.net/> (last visited May 10, 2022).

¹⁸ See Ex 1.

individuals. On April 4, 2022, ARcare concluded the review and determined that personal information relating to individuals was in affected files.

What Information Was Involved?

Though it varies by individual, the types of personal and/or medical information that may have been accessed or acquired by the unauthorized actor included: names, Social Security numbers, drivers license or state identification numbers, dates of birth, financial account information, medical treatment information, prescription information, medical diagnosis or condition information, and health insurance information. At this time, ARcare is unaware of any or actual or attempted misuse of the affected information as a result of this incident.

What We Are Doing.

ARcare treats its responsibility to safeguard information in its care as an utmost priority. As such, ARcare responded immediately to this incident and have been working diligently to provide you with an accurate and complete notice of the incident as soon as possible. As part of its ongoing commitment to the privacy and security of personal information in its care, ARcare is reviewing and updating existing policies and procedures relating to data protection and security. ARcare is also investigating additional security measures to mitigate any risk associated with this incident and to better prevent future similar incidents. On April 25, 2022, ARcare began providing notice of this incident to potentially impacted individuals and to regulators where required.

What You Can Do.

Although ARcare is unaware of the misuse of any personal information impacted by this incident, individuals are encouraged to remain vigilant against events of identity theft by reviewing account statements, explanation of benefits, and monitoring free credit reports for suspicious activity and to detect errors. Any suspicious activity should be reported to the appropriate insurance company, health care provider, or financial institution.¹⁹

32. The Website Notice confirms that the types of PII accessed and/or acquired by the unauthorized actor included: names, Social Security numbers, driver's license or state

¹⁹ Ex. 1.

identification numbers, dates of birth, financial account information, medical treatment information, prescription information, medical diagnosis or condition information, and health insurance information.

33. On or about April 25, 2022, Defendant notified U.S. Department of Health and Human Services Office for Civil Rights (“HHS”) and the Massachusetts Attorney General of the Data Breach.²⁰ Defendant reported to HHS that the unredacted PHI of over 345,000 individuals was compromised in the Data Breach.

34. In response to the Data Breach, Defendant claims that “[a]s part of its ongoing commitment to the privacy and security of personal information in its care, ARcare is reviewing and updating existing policies and procedures relating to data protection and security.”²¹ Defendant also states it “is also investigating additional security measures to mitigate any risk associated with this incident and to better prevent future similar incidents.”²² However, the details of the root cause of the Data Breach, the vulnerabilities exploited, and the remedial measures undertaken to ensure a breach does not occur again have not been shared with regulators or Plaintiff and Class Members, who retain a vested interest in ensuring that their information remains protected.

35. Plaintiff’s and Class Members’ unencrypted information may end up for sale on the dark web, or simply fall into the hands of companies that will use the detailed PII and/or PHI for targeted marketing without the approval of Plaintiff and Class Members. Unauthorized individuals can easily access the PII and PHI of Plaintiff and Class Members.

36. Defendant did not use reasonable security procedures and practices appropriate to the nature of the sensitive, unencrypted information it was maintaining for Plaintiff and Class

²⁰ Exhibit 3 (Sample Notice of Data Breach Letter provided to the Massachusetts Attorney General).

²¹ Ex. 1.

²² Ex. 1.

Members, causing their PII and PHI to be exposed.

Defendant Acquires, Collects and Stores Plaintiff's and Class Members' PII and PHI.

37. Defendant acquired, collected, and stored Plaintiff's and Class Members' PII and PHI.

38. As a condition of its relationships with Plaintiff and Class Members, Defendant required that Plaintiff and Class Members entrust Defendant with highly confidential PII and PHI.

39. By obtaining, collecting, and storing the PII and PHI of Plaintiff and Class Members, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting the PII and PHI from disclosure.

40. Plaintiff and Class Members have taken reasonable steps to maintain the confidentiality of their PII and PHI and relied on Defendant to keep their PII and PHI confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

Securing PII and Preventing Breaches

41. Defendant could have prevented this Data Breach by properly securing and encrypting the PII and PHI of Plaintiff and Class Members. Alternatively, Defendant could have destroyed the data, especially years-old data from former patients.

42. Defendant's negligence in safeguarding the PII of Plaintiff and Class Members is exacerbated by the repeated warnings and alerts directed to protecting and securing sensitive data.

43. Despite the prevalence of public announcements of data breach and data security compromises Defendant failed to take appropriate steps to protect the PII and PHI of Plaintiff and Class Members from being compromised.

44. The Federal Trade Commission ("FTC") defines identity theft as "a fraud

committed or attempted using the identifying information of another person without authority.”²³ 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.”²⁴

45. The ramifications of Defendant’s failure to keep secure the PII of Plaintiff and Class Members are long lasting and severe. Once PII is stolen, particularly Social Security numbers, fraudulent use of that information and damage to victims may continue for years.

Value of Personal Identifiable Information

46. The PII 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, personal information can be sold at a price ranging from \$40 to \$200, and bank details have a price range of \$50 to \$200.²⁵ Experian reports that a stolen credit or debit card number can sell for \$5 to \$110 on the dark web.²⁶ Criminals can also purchase access to entire company data breaches from \$900 to \$4,500.²⁷

47. Social Security numbers, for example, are among the worst kind of personal information to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change. The Social Security Administration stresses that the loss of an

²³ 17 C.F.R. § 248.201 (2013).

²⁴ *Id.*

²⁵ *Your personal data is for sale on the dark web. Here’s how much it costs*, Digital Trends, Oct. 16, 2019, available at: <https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/> (last visited May 10, 2022).

²⁶ *Here’s How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, available at: <https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/> (last visited May 10, 2022).

²⁷ *In the Dark*, VPNOverview, 2019, available at: <https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/> (last visited May 10, 2022).

individual's Social Security number, as is the case here, can lead to identity theft and extensive financial fraud:

A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.²⁸

48. What is more, it is no easy task to change or cancel a stolen Social Security number.

An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

49. Even then, a new Social Security number may not be effective. According to Julie Ferguson of the Identity Theft Resource Center, "The credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."²⁹

50. Further, there is a market for Plaintiff's and Class Members' PHI, and the stolen PHI has inherent value. Sensitive healthcare data can sell for as much as \$363 per record according to the Infosec Institute.³⁰

51. PHI is particularly valuable because criminals can use it to target victims with

²⁸ SOCIAL SECURITY ADMINISTRATION, *Identity Theft and Your Social Security Number*, available at: <https://www.ssa.gov/pubs/EN-05-10064.pdf> (last visited May 10, 2022).

²⁹ Bryan Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), available at: <http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millionsworrying-about-identity-theft> (last visited May 10, 2022).

³⁰ See 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 10, 2022).

frauds and scams that take advantage of the victim's medical conditions or victim settlements. It can be used to create fake insurance claims, allowing for the purchase and resale of medical equipment, or gain access to prescriptions for illegal use or resale. Drug manufacturers, medical device manufacturers, pharmacies, hospitals, and other healthcare service providers often purchase PII and 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.

52. Medical identify theft can result in inaccuracies in medical records and costly false claims. It can also have life-threatening consequences. If a victim's health information is mixed with other records, it can lead to misdiagnosis or mistreatment. "Medical identity theft is a growing and dangerous crime that leaves its victims with little to no recourse for recovery," reported Pam Dixon, executive director of World Privacy Forum. "Victims often experience financial repercussions and worse yet, they frequently discover erroneous information has been added to their personal medical files due to the thief's activities."³¹

53. Similarly, the FBI Cyber Division, in an April 8, 2014, Private Industry Notification, advised:

Cyber criminals are selling [medical] information on the black market at a rate of \$50 for each partial EHR, compared to \$1 for a stolen social security number or credit card number. EHR can then be used to file fraudulent insurance claims, obtain prescription medication, and advance identity theft. EHR theft is also more difficult to detect, taking almost twice as long as normal identity theft.³²

54. Based on the foregoing, the information actually or potentially compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information

³¹ Michael Ollove, "The Rise of Medical Identity Theft in Healthcare," KAISER HEALTH NEWS (Feb. 7, 2014) available at: <https://khn.org/news/rise-of-identity-theft/> (last visited May 10, 2022).

³² FBI CYBER DIVISION, *Private Industry Notification*, "(U) Health Care Systems and Medical Devices at Risk for Increased Cyber Intrusions for Financial Gain," Apr. 8, 2014, available at: <http://www.illumweb.com/wp-content/uploads/ill-mo-uploads/103/2418/health-systems-cyber-intrusions.pdf> (last visited May 10, 2022)

in a retailer data breach because, there, victims can cancel or close credit and debit card accounts. The information actually or potentially compromised in this Data Breach is impossible to “close” and difficult, if not impossible, to change—name, Social Security number, medical records, and potentially date of birth.

55. 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.”³³

56. Among other forms of fraud, identity thieves may obtain driver’s licenses, government benefits, medical services, and housing or even give false information to police.

57. The PII and PHI of Plaintiff and Class Members was taken by hackers to engage in identity theft or and or to sell it to other criminals who will purchase the PII and PHI for that purpose. The fraudulent activity resulting from the Data Breach may not come to light for years.

58. There may be a time lag between when harm occurs versus when it is discovered, and also between when PII and PHI is stolen and when it is used. According to the U.S. Government Accountability Office (“GAO”), which conducted a study regarding data breaches:

[L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.³⁴

59. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the PII and PHI of Plaintiff and Class Members, including Social Security numbers and/or dates of birth, and of the foreseeable consequences that would occur if

³³ Time Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, (Feb. 6, 2015), available at: <https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html> (last visited May 10, 2022).

³⁴ *Report to Congressional Requesters*, GAO, at 29 (June 2007), available at: <https://www.gao.gov/products/gao-07-737> (last visited May 10, 2022).

the PII was compromised, including, specifically, the significant costs that would be imposed on Plaintiff and Class Members a result.

60. Plaintiff and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. Plaintiff and Class Members are incurring and will continue to incur such damages in addition to any fraudulent use of their PII and PHI.

61. Defendant was, or should have been, fully aware of the unique type and the significant volume of data stored on and/or shared on its system, amounting to more than 345,353 individuals' detailed, personal information and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

62. To date, Defendant has offered Plaintiff and Class Members only one year of credit and CyberScan monitoring and identity theft recovery services through IDX. The offered service is inadequate to protect Plaintiff and Class Members from the threats they face for years to come, particularly in light of the PII and PHI at issue here.

63. The injuries to Plaintiff and Class Members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for the PII and PHI of Plaintiff and Class Members.

Defendant's Conduct Violates HIPAA

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 has subsequently promulgated five rules under authority of the Administrative Simplification provisions of HIPAA.

65. Defendant's Data Breach resulted from a combination of insufficiencies that

indicate Defendant failed to comply with safeguards mandated by HIPAA regulations and industry standards. First, it can be inferred from Defendant's Data Breach that Defendant either failed to implement, or inadequately implemented, information security policies or procedures in place to protect Plaintiff and Class Members' PII and PHI.

66. In addition, Defendant's Data Breach could have been prevented if Defendant implemented HIPAA mandated, industry standard policies and procedures for securely disposing of PII and PHI when it was no longer necessary and/or had honored its obligations to its patients.

67. Defendant's security failures also include, but are not limited to:

- a. Failing to maintain an adequate data security system to prevent data loss;
- b. Failing to mitigate the risks of a data breach and loss of data;
- c. Failing to ensure the confidentiality and integrity of electronic protected health information Defendant creates, receives, maintains, and transmits in violation of 45 CFR 164.306(a)(1);
- d. Failing to implement 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 in violation of 45 CFR 164.312(a)(1);
- e. Failing to implement policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 CFR 164.308(a)(1);
- f. Failing to identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity in violation of 45 CFR 164.308(a)(6)(ii);
- g. Failing to protect against any reasonably-anticipated threats or hazards to the security or integrity of electronic protected health information in violation of 45

CFR 164.306(a)(2);

- h. Failing to protect against any reasonably-anticipated uses or disclosures of electronic protected health information that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 CFR 164.306(a)(3);
- i. Failing to ensure compliance with HIPAA security standard rules by Defendant's workforce in violation of 45 CFR 164.306(a)(94);
- j. Impermissibly and improperly using and disclosing protected health information that is and remains accessible to unauthorized persons in violation of 45 CFR 164.502, *et seq.*; and
- k. Retaining information past a recognized purpose and not deleting it.

68. The HIPAA Breach Notification Rule, 45 CFR §§ 164.400-414, also required Defendant to provide notice of the breach to each affected individual “without unreasonable delay and *in no case later than 60 days following discovery of the breach.*”³⁵

69. Because Defendant has failed to comply with industry standards, while monetary relief may cure some of Plaintiff and Class Members' injuries, injunctive relief is necessary to ensure Defendant's approach to information security is adequate and appropriate. Defendant still maintains the protected health information and other PII of Plaintiff and Class Members; and without the supervision of the Court via injunctive relief, Plaintiff and Class Members' protected health information and other PII remains at risk of subsequent Data Breaches.

ARcare Failed to Comply with FTC Guidelines

70. Defendant was also prohibited by the Federal Trade Commission Act (“FTC Act”)

³⁵ Breach Notification Rule, U.S. DEP'T OF HEALTH & HUMAN SERVICES, *available at: [hhs.gov/hipaa/for-professionals/breach-notification/index.html](https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html)* (emphasis added) (last visited May 10, 2022).

(15 U.S.C. §45) from engaging in “unfair or deceptive acts or practices in or affecting commerce.” The Federal Trade Commission (“FTC”) has concluded that a company’s failure to maintain reasonable and appropriate data security for consumers’ sensitive personal information is an “unfair practice” in violation of the FTC Act. *See, e.g., FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015).

71. The Federal Trade Commission (“FTC”) has promulgated numerous guides for businesses that highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.³⁶

72. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cybersecurity guidelines for businesses.³⁷ The guidelines note that businesses should protect the personal customer 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 any security problems.

73. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to private 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.³⁸

³⁶ Federal Trade Commission, *Start With Security: A Guide for Business*, available at: <https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf> (last visited May 10, 2022).

³⁷ Federal Trade Commission, *Protecting Personal Information: A Guide for Business*, available at: https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited May 10, 2022).

³⁸ FTC, *Start With Security*, *supra*.

74. 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.

75. Defendant failed to properly implement basic data security practices. Defendant’s failure to employ reasonable and appropriate measures to protect against unauthorized access to patient PII and PHI constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

76. Defendant was at all times fully aware of its obligation to protect the PII and PHI of its current and former patients because of its status as a leading healthcare provider. Defendant was also aware of the significant repercussions that would result from its failure to do so.

Plaintiff Jessica White’s Experience

77. Plaintiff Jessica White is a patient of ARcare, a relationship which required that Plaintiff produce her Social Security number, among other personal and medical information, to Defendant.

78. In or around April 2022, Plaintiff received letters from a physician’s office in another county. These letters included invoices for healthcare services that Plaintiff had never received nor requested, yet the invoices included her name and address for billing purposes.

79. On or around May 1, 2022, Plaintiff received a Notice of Data Breach from Defendant.³⁹ The Notice of Data Breach Letter, dated April 25, 2022, stated that the “information present in the files that were accessed and/or acquired as a result of the incident may have included

³⁹ Exhibit 4 (Plaintiff’s Notice of Data Privacy Incident Letter).

your date of birth, Social Security Number, medical treatment information, prescription information, medical diagnosis or condition information, health insurance information, and name.”⁴⁰

80. As a result of the Data Breach, Plaintiff spent time dealing with the consequences of the Data Breach, which includes time spent on the telephone and sorting through her unsolicited emails, verifying the legitimacy of the Data Breach, exploring credit monitoring and identity theft insurance options, attempting to enroll in the credit monitoring and identity theft protection services offered by Defendant, and self-monitoring her accounts. This time has been lost forever and cannot be recaptured.

81. Additionally, Plaintiff is very careful about sharing her PII. She has never knowingly transmitted unencrypted PII over the internet or any other unsecured source.

82. Plaintiff stores any documents containing her PII and PHI in a safe and secure location. Moreover, she diligently chooses unique usernames and passwords for her few online accounts.

83. Plaintiff’s sensitive information, including her name and address, among other PHI and PII belonging to Plaintiff, has already been used by an unauthorized individual to obtain and bill healthcare services in Plaintiff’s name.

84. Further, Plaintiff suffered actual injury in the form of damages to and diminution in the value of her PII and PHI—a form of intangible property that Plaintiff entrusted to Defendant for the purpose of obtaining healthcare from Defendant, which was actually or potentially compromised in and as a result of the Data Breach.

85. Plaintiff suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of her privacy.

⁴⁰ *Id.*

86. Plaintiff has suffered injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from her PII and PHI, especially her Social Security number, in combination with her name, being placed in the hands of unauthorized third-parties and possibly criminals. Plaintiff has also suffered identity theft as a result of her PII and PHI being placed in the hands of unauthorized third-parties, who used that PII and PHI to unlawfully obtain medical treatment in her name.

87. Plaintiff has a continuing interest in ensuring that her PII, which, upon information and belief, remain backed up in Defendant's possession, is protected and safeguarded from future breaches.

V. CLASS ALLEGATIONS

88. Plaintiff brings this nationwide class action on behalf of herself and on behalf of all others similarly situated pursuant to Rule 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure.

89. The Nationwide Class that Plaintiff seeks to represent is defined as follows:

All individuals residing in the United States whose PII and/or PHI was actually or potentially compromised during the period of unauthorized access to ARcare's computer systems as referenced in the Notice of Data Privacy Incident ARcare sent to Plaintiff and other Class Members on or around April 25, 2022 (the "Nationwide Class").

90. Excluded from the Classes are the following individuals and/or entities: Defendant and Defendant's parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendant has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; any and all federal, state or local governments, including but not limited to their departments, agencies, divisions, bureaus, boards, sections, groups, counsels and/or subdivisions; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members and staff members.

91. Plaintiff reserves the right to modify or amend the definition of the proposed classes before the Court determines whether certification is appropriate.

92. This action is brought and may be maintained as a class action because there is a well-defined community of interest among many persons who comprise a readily ascertainable class. A well-defined community of interest exists to warrant classwide relief because Plaintiff and all members of the Nationwide Class were subjected to the same wrongful practices by Defendant, entitling them to the same relief.

93. The Nationwide Class is so numerous that individual joinder of its members is impracticable. While the exact number of Class Members is unknown to Plaintiff at this time, Plaintiff is informed and believes that there are at least tens of thousands of Class Members. Defendant advised the U.S. Department of Health and Human Services Office for Civil Rights that the Data Breach affected 345,353 individuals.⁴¹

94. Common questions of law and fact exist as to members of the Nationwide Class and predominate over any questions which affect only individual members of the Class. These common questions include, but are not limited to:

- a. Whether and to what extent Defendant had a duty to protect the PII and PHI of Plaintiff and Class Members;
- b. Whether Defendant had a duty not to disclose the PII and PHI of Plaintiff and Class Members to unauthorized third parties;
- c. Whether Defendant had a duty not to use the PII and PHI of Plaintiff and Class Members for non-business purposes;
- d. Whether Defendant failed to adequately safeguard the PII and PHI of Plaintiff and Class Members;

⁴¹ https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (last visited May 10, 2022).

- e. Whether and when Defendant actually learned of the Data Breach;
- f. Whether Defendant adequately, promptly, and accurately informed Plaintiff and Class Members that their PII and PHI had been actually or potentially compromised;
- g. Whether Defendant violated the law by failing to promptly notify Plaintiff and Class Members that their PII and PHI had been actually or potentially compromised;
- h. 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;
- i. Whether Defendant adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;
- j. Whether Plaintiff and Class Members are entitled to actual, damages, and/or statutory damages as a result of Defendant's wrongful conduct;
- k. Whether Plaintiff and Class Members are entitled to restitution as a result of Defendant's wrongful conduct; and
- l. Whether Plaintiff and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach.

95. Plaintiff is a member of the Classes she seeks to represent, and her claims and injuries are typical of the claims and injuries of the other Class Members.

96. Plaintiff will adequately and fairly protect the interests of other Class Members. Plaintiff has no interests adverse to the interests of absent Class Members. Plaintiff is represented by legal counsel with substantial experience in class action litigation. The interests of Class Members will be fairly and adequately protected by Plaintiff and her counsel.

97. Defendant has acted or refused to act on grounds that apply generally to the Class Members, so that final injunctive relief or corresponding declaratory relief is appropriate

respecting the Class as a whole.

98. A class action is superior to other available means for fair and efficient adjudication of the claims of the Class and would be beneficial for the parties and the court. Class action treatment will allow a large number of similarly situated persons to prosecute their common claims in a single forum, simultaneously, efficiently, and without the unnecessary duplication of effort and expense that numerous individual actions would require. The amounts owed to the many individual Class Members are likely to be relatively small, and the burden and expense of individual litigation would make it difficult or impossible for individual members of the class to seek and obtain relief. A class action will serve an important public interest by permitting such individuals to effectively pursue recovery of the sums owed to them. Further, class litigation prevents the potential for inconsistent or contradictory judgments raised by individual litigation. Plaintiff is unaware of any difficulties that are likely to be encountered in the management of this action that would preclude its maintenance as a class action.

COUNT I
Negligence
(On Behalf of Plaintiff and the Nationwide Class)

99. Plaintiff and the Nationwide Class re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 98.

100. Plaintiff and the Nationwide Class provided and entrusted Defendant with certain PII and PHI, including, without limitation, names, Social Security numbers, driver's license or state identification numbers, dates of birth, financial account information, medical treatment information, prescription information, medical diagnosis or condition information, and health insurance information.

101. Plaintiff and the Nationwide Class entrusted their PII and PHI to Defendant on the premise and with the understanding that Defendant would safeguard their information, use their

PII and PHI for business purposes only, and/or not disclose their PII and PHI to unauthorized third parties.

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

103. Defendant knew or reasonably should have known that the failure to exercise due care in the collecting, storing, and using of the PII and PHI of Plaintiff and the Nationwide Class involved an unreasonable risk of harm to Plaintiff and the Nationwide Class, even if the harm occurred through the criminal acts of a third party.

104. Defendant had a duty to exercise reasonable care in safeguarding, securing, and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties. This duty includes, among other things, designing, maintaining, and testing Defendant's security protocols to ensure that the PII and PHI of Plaintiff and the Nationwide Class in Defendant's possession was adequately secured and protected.

105. Defendant also had a duty to exercise appropriate clearinghouse practices to remove PII and PHI it was no longer required to retain pursuant to regulations, including that of former customers or patients.

106. Defendant also had a duty to have procedures in place to detect and prevent the improper access and misuse of the PII and PHI of Plaintiff and the Nationwide Class.

107. Defendant's duty to use reasonable security measures arose as a result of the special relationship that existed between Defendant and Plaintiff and the Nationwide Class. That special relationship arose because Plaintiff and the Nationwide Class entrusted Defendant with their confidential PII and PHI, a necessary part of their relationships with Defendant.

108. Defendant was subject to an "independent duty," untethered to any contract

between Defendant and Plaintiff or the Nationwide Class.

109. A breach of security, unauthorized access, and resulting injury to Plaintiff and the Nationwide Class was reasonably foreseeable, particularly in light of Defendant's inadequate security practices and Defendant's previous data breach, just last year.

110. Plaintiff and the Nationwide Class were the foreseeable and probable victims of any inadequate security practices and procedures. Defendant knew or should have known of the inherent risks in collecting and storing the PII and PHI of Plaintiff and the Nationwide Class, the critical importance of providing adequate security of that PII and PHI, and the necessity for encrypting PII and PHI stored on Defendant's systems.

111. Defendant's own conduct created a foreseeable risk of harm to Plaintiff and the Nationwide Class. Defendant's misconduct included, but was not limited to, its failure to take the steps and opportunities to prevent the Data Breach as set forth herein. Defendant's misconduct also included its decisions not to comply with industry standards for the safekeeping of the PII and PHI of Plaintiff and the Nationwide Class, including basic encryption techniques freely available to Defendant.

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

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

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

parties.

115. Defendant had a duty to employ proper procedures to prevent the unauthorized dissemination of the PII and PHI of Plaintiff and the Nationwide Class.

116. Defendant has admitted that the PII and PHI of Plaintiff and the Nationwide Class was wrongfully lost and disclosed to unauthorized third persons as a result of the Data Breach.

117. Defendant, through its actions and/or omissions, unlawfully breached its duties to Plaintiff and the Nationwide Class by failing to implement industry protocols and exercise reasonable care in protecting and safeguarding the PII and PHI of Plaintiff and the Nationwide Class during the time the PII and PHI was within Defendant's possession or control.

118. Defendant improperly and inadequately safeguarded the PII and PHI of Plaintiff and the Nationwide Class in deviation of standard industry rules, regulations, and practices at the time of the Data Breach.

119. Defendant failed to heed industry warnings and alerts to provide adequate safeguards to protect the PII and PHI of Plaintiff and the Nationwide Class in the face of increased risk of theft.

120. Defendant, through its actions and/or omissions, unlawfully breached its duty to Plaintiff and the Nationwide Class by failing to have appropriate procedures in place to detect and prevent dissemination of their PII and PHI.

121. Defendant breached its duty to exercise appropriate clearinghouse practices by failing to remove PII and PHI it was no longer required to retain pursuant to regulations.

122. Defendant, through its actions and/or omissions, unlawfully breached its duty to adequately and timely disclose to Plaintiff and the Nationwide Class the existence and scope of the Data Breach.

123. But for Defendant's wrongful and negligent breach of duties owed to Plaintiff and

the Nationwide Class, the PII and PHI of Plaintiff and the Nationwide Class would not have been actually or potentially compromised.

124. There is a close causal connection between Defendant's failure to implement security measures to protect the PII and PHI of Plaintiff and the Nationwide Class and the harm, or risk of imminent harm, suffered by Plaintiff and the Nationwide Class. The PII and PHI of Plaintiff and the Nationwide Class was actually or potentially compromised as the proximate result of Defendant's failure to exercise reasonable care in safeguarding such PII and PHI by adopting, implementing, and maintaining appropriate security measures.

125. Additionally, Section 5 of the FTC Act 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 PII and PHI. The FTC publications and orders described above also form part of the basis of Defendant's duty in this regard.

126. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect 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 obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiff and the Nationwide Class.

127. Defendant's violation of Section 5 of the FTC Act constitutes negligence *per se*.

128. Plaintiff and the Nationwide Class are within the class of persons that the FTC Act was intended to protect.

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

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

130. As a direct and proximate result of Defendant's negligence and negligence *per se*, Plaintiff and the Nationwide Class have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity of how their PII and PHI is used; (iii) the compromise, publication, and/or theft of their PII and PHI; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII and PHI; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their PII and PHI, which remain in Defendant's possession and are subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII and PHI of Plaintiff and the Nationwide Class; and (viii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII and PHI compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and the Nationwide Class.

131. Defendant's violation of HIPAA also independently constitutes negligence *per se*.

132. HIPAA privacy laws were enacted with the objective of protecting the confidentiality of patients' healthcare information and set forth the conditions under which such information can be used, and to whom it can be disclosed. HIPAA privacy laws not only apply to healthcare providers and the organizations they work for, but to any entity that may have access to healthcare information about a patient that—if it were to fall into the wrong hands—could present a risk of harm to the patient's finances or reputation.

133. Plaintiff and the Nationwide Class are within the class of persons that HIPAA

privacy laws were intended to protect.

134. The harm that occurred as a result of the Data Breach is the type of harm HIPAA privacy laws were intended to guard against.

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

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

137. As a direct and proximate result of Defendant's negligence and negligence *per se*, Plaintiff and the Nationwide Class are entitled to and demand actual, consequential, and nominal damages.

COUNT II
Breach of Implied Contract
(On Behalf of Plaintiff and the Nationwide Class)

138. Plaintiff and the Nationwide Class re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 98.

139. Defendant required Plaintiff and the Nationwide Class to provide and entrust their PII and PHI, including, without limitation, names, Social Security numbers, driver's license or state identification numbers, dates of birth, financial account information, medical treatment information, prescription information, medical diagnosis or condition information, and health insurance information as a condition of obtaining medical care from Defendant.

140. Defendant's "Privacy Policy" provides, in part, that Defendant is "committed to protecting your personal health information."

141. Defendant solicited and invited Plaintiff and Class Members to provide their PII and PHI as part of Defendant's regular business practices. Plaintiff and Class Members accepted Defendant's offers and provided their PII and PHI to Defendant.

142. As a condition of receiving care from Defendant, Plaintiff and the Nationwide Class provided and entrusted their personal information to Defendant. In so doing, Plaintiff and the Nationwide Class entered into implied contracts 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 the Nationwide Class if their data had been breached and compromised or stolen.

143. A meeting of the minds occurred when Plaintiff and the Nationwide Class Members agreed to, and did, provide their PII and PHI to Defendant, in exchange for, amongst other things, the protection of their PII and PHI.

144. Plaintiff and the Nationwide Class fully performed their obligations under the implied contracts with Defendant.

145. Defendant breached the implied contracts it made with Plaintiff and the Nationwide Class by failing to safeguard and protect their personal and financial information and by failing to provide timely and accurate notice to them that personal and financial information was compromised as a result of the data breach.

146. As a direct and proximate result of Defendant's above-described breach of implied contract, Plaintiff and the Nationwide Class have suffered (and will continue to suffer) ongoing, imminent, and impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and abuse, resulting in monetary loss

and economic harm; loss of the confidentiality of the stolen confidential data; the illegal sale of the compromised data on the dark web; expenses and/or time spent on credit monitoring and identity theft insurance; time spent scrutinizing bank statements, credit card statements, and credit reports; expenses and/or time spent initiating fraud alerts, decreased credit scores and ratings; lost work time; and other economic and non-economic harm.

147. As a result of Defendant's breach of implied contract, Plaintiff and the Nationwide Class are entitled to and demand actual, consequential, and nominal damages.

COUNT III
Invasion of Privacy
(On Behalf of Plaintiff and the Nationwide Class)

148. Plaintiff and the Nationwide Class re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 98.

149. Plaintiff and the Nationwide Class had a legitimate expectation of privacy to their PII and PHI and were entitled to the protection of this information against disclosure to unauthorized third parties.

150. Defendant owed a duty to its current and former patients, including Plaintiff and the Nationwide Class, to keep their PII and PHI contained as a part thereof, confidential.

151. Defendant failed to protect and released to unknown and unauthorized third parties the PII and PHI of Plaintiff and the Nationwide Class.

152. Defendant allowed unauthorized and unknown third parties to access and examine of the PII and PHI of Plaintiff and the Nationwide Class, by way of Defendant's failure to protect the PII and PHI.

153. The unauthorized release to, custody of, and examination by unauthorized third parties of the PII and PHI of Plaintiff and the Nationwide Class is highly offensive to a reasonable person.

154. The intrusion was into a place or thing, which was private and is entitled to be private. Plaintiff and the Nationwide Class disclosed their PII and PHI to Defendant as part of Plaintiff's and the Nationwide Class's relationships with Defendant, but privately with an intention that the PII and PHI would be kept confidential and would be protected from unauthorized disclosure. Plaintiff and the Nationwide Class were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization.

155. The Data Breach at the hands of Defendant constitutes an intentional interference with Plaintiff's and the Nationwide Class's interest in solitude or seclusion, either as to their persons or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

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

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

158. As a proximate result of the above acts and omissions of Defendant, the PII and PHI of Plaintiff and the Nationwide Class was disclosed to third parties without authorization, causing Plaintiff and the Nationwide Class to suffer damages.

159. Unless and until enjoined, and restrained by order of this Court, Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiff and the Nationwide Class in that the PII and PHI maintained by Defendant can be viewed, distributed, and used by unauthorized persons for years to come. Plaintiff and the Nationwide Class have no

adequate remedy at law for the injuries in that a judgment for monetary damages will not end the invasion of privacy for Plaintiff and the Nationwide Class.

COUNT IV
Breach of Confidence
(On Behalf of Plaintiff and the Nationwide Class)

160. Plaintiff and the Nationwide Class re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 98.

161. At all times during Plaintiff's and the Nationwide Class's interactions with Defendant, Defendant was fully aware of the confidential and sensitive nature of Plaintiff's and the Nationwide Class's PII and PHI that Plaintiff and the Nationwide Class provided to Defendant.

162. As alleged herein and above, Defendant's relationship with Plaintiff and the Nationwide Class was governed by terms and expectations that Plaintiff's and the Nationwide Class's PII and PHI would be collected, stored, and protected in confidence, and would not be disclosed to unauthorized third parties.

163. Plaintiff and the Nationwide Class provided their PII and PHI to Defendant with the explicit and implicit understandings that Defendant would protect and not permit the PII and PHI to be disseminated to any unauthorized third parties.

164. Plaintiff and the Nationwide Class also provided their PII and PHI to Defendant with the explicit and implicit understandings that Defendant would take precautions to protect that PII and PHI from unauthorized disclosure.

165. Defendant voluntarily received in confidence the PII and PHI of Plaintiff and the Nationwide Class with the understanding that PII and PHI would not be disclosed or disseminated to the public or any unauthorized third parties.

166. Due to Defendant's failure to prevent and avoid the Data Breach from occurring, the PII and PHI of Plaintiff and the Nationwide Class was disclosed and misappropriated to

unauthorized third parties beyond Plaintiff's and the Nationwide Class's confidence, and without their express permission.

167. As a direct and proximate cause of Defendant's actions and/or omissions, Plaintiff and the Nationwide Class have suffered damages.

168. But for Defendant's disclosure of Plaintiff's and the Nationwide Class's PII and PHI in violation of the parties' understanding of confidence, their PII and PHI would not have been actually or potentially compromised by unauthorized third parties. The Data Breach was the direct and legal cause of the theft of Plaintiff's and the Nationwide Class's PII and PHI as well as the resulting damages.

169. The injury and harm Plaintiff and the Nationwide Class suffered was the reasonably foreseeable result of Defendant's unauthorized disclosure of Plaintiff's and the Nationwide Class's PII and PHI. Defendant knew or should have known its methods of accepting and securing Plaintiff's and the Nationwide Class's PII and PHI was inadequate as it relates to, at the very least, securing servers and other equipment containing Plaintiff's and the Nationwide Class's PII and PHI.

170. As a direct and proximate result of Defendant's breach of its confidence with Plaintiff and the Nationwide Class, Plaintiff and the Nationwide Class have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity how their PII and PHI is used; (iii) the compromise, publication, and/or theft of their PII and PHI; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII and PHI; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with

placing freezes on credit reports; (vii) the continued risk to their PII and PHI, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII and PHI of Plaintiff and the Nationwide Class; and (viii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII and PHI compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and the Nationwide Class.

171. As a direct and proximate result of Defendant's breaches of confidence, Plaintiff and the Nationwide Class have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

172. As a result of Defendant's breaches of confidence, Plaintiff and the Nationwide Class are entitled to and demand actual, consequential, and nominal damages.

PRAYER FOR RELIEF

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

- A. For an Order certifying the Nationwide Class, and appointing Plaintiff and her Counsel to represent such Class;
- B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of the PII and PHI of Plaintiff and Class Members, and from refusing to issue prompt, complete, any 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 personal identifying information 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 systems 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 its 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 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 personal identifying information 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 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, and to report any deficiencies with compliance of the Court's final judgment;

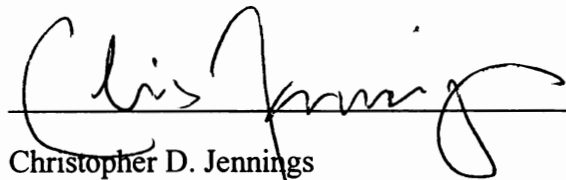
- D. For an award of damages, including actual, consequential, nominal, and statutory damages, as allowed by law in an amount to be determined;
- E. For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;
- F. For prejudgment interest on all amounts awarded; and
- G. Such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiff hereby demands that this matter be tried before a jury.

Date: May 16, 2022

Respectfully Submitted,



Christopher D. Jennings
Arkansas Bar No. 2006306
Nathan I. Reiter III
Arkansas Bar No. 2021205
JOHNSON FIRM

610 President Clinton Avenue, Suite 300
Little Rock, Arkansas 72201
Telephone: (501) 372-1300
Facsimile: (888) 505-0909
chris@yourattorney.com
nathan@yourattorney.com

JEAN S. MARTIN
(Pro Hac Vice application forthcoming)
FRANCESCA KESTER
(Pro Hac Vice application forthcoming)
**MORGAN & MORGAN COMPLEX
LITIGATION GROUP**
201 N. Franklin Street, 7th Floor
Tampa, Florida 33602
(813) 559-4908
jean.martin@ForThePeople.com
fkester@ForThePeople.com

Attorneys for Plaintiff and the Putative Class

EXHIBIT 1

NOTICE OF DATA PRIVACY INCIDENT

ARcare is notifying certain individuals of a recent data privacy incident that may impact the privacy of a limited amount of personal and/or medical information. ARcare is unaware of any misuse of individual information and is providing notice to potentially affected individuals out of an abundance of caution.

About the Incident

On February 24, 2022, ARcare experienced a data security incident that impacted its computer systems and caused a temporary disruption to services. ARcare immediately worked to secure its systems and quickly commenced an investigation to confirm the nature and scope of the incident. On March 14, 2022, the investigation determined that an unauthorized actor may have accessed and/or acquired some sensitive data during a period of unauthorized access to ARcares computer systems between January 18, 2022 and February 24, 2022. A thorough review of the contents of the affected data was subsequently performed to determine whether it contained any sensitive information and identify affected individuals. On April 4, 2022, ARcare concluded the review and determined that personal information relating to individuals was in affected files.

What Information Was Involved?

Though it varies by individual, the types of personal and/or medical information that may have been accessed or acquired by the unauthorized actor included: names, Social Security numbers, drivers license or state identification numbers, dates of birth, financial account information, medical treatment information, prescription information, medical diagnosis or condition information, and health insurance information. At this time, ARcare is unaware of any or actual or attempted misuse of the affected information as a result of this incident.

What We Are Doing.

ARcare treats its responsibility to safeguard information in its care as an utmost priority. As such, ARcare responded immediately to this incident and have been working diligently to provide you with an accurate and complete notice of the incident as soon as possible. As part of its ongoing commitment to the privacy and security of personal information in its care, ARcare is reviewing and updating existing policies and procedures relating to data protection and security. ARcare is also investigating additional security measures to mitigate any risk associated with this incident and to better prevent future similar incidents. On April 25, 2022, ARcare began providing notice of this incident to potentially impacted individuals and to regulators where required.

What You Can Do.

Although ARcare is unaware of the misuse of any personal information impacted by this incident, individuals are encouraged to remain vigilant against events of identity theft by reviewing account statements, explanation of benefits, and monitoring free credit reports for suspicious activity and to detect errors. Any suspicious activity should be reported to the appropriate insurance company, health care provider, or financial institution.

For More Information

Individuals seeking additional information regarding this incident can call ARcares dedicated, toll-free number at (833) 783-1354, available Monday through Friday from 8am to 8pm Central time. Individuals may also write to ARcare directly at: 117 S. 2nd Street, Augusta, Arkansas 72006. ARcare is committed to safeguarding personal information and will continue to work to enhance the protections in place to secure the information in its care.

BEST PRACTICES

Although ARcare is unaware of any misuse of personal information as a result of this incident, individuals are encouraged to remain vigilant against incidents of identity theft and fraud, to review account statements, explanation of benefits, and to monitor credit reports for suspicious activity and to detect errors. Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also directly contact the three major credit reporting bureaus listed below to request a free copy of your credit report.

Consumers have the right to place an initial or extended fraud alert on a credit file at no cost. An initial fraud alert is a one-year alert that is placed on a consumers credit file. Upon seeing a fraud alert display on a consumers credit file, a business is required to take steps to verify the consumers identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a credit freeze on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumers express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a credit freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. To request a credit freeze, you will need to provide the following information:

1. Full name (including middle initial, as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state drivers license or ID card, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if you are a victim of identity theft.

Should you wish to place a fraud alert or a credit freeze, please contact the three major credit reporting bureaus listed below:

Equifax	Experian	TransUnion
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
1-888-298-0045	1-888-397-3742	1-833-395-6938
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Additional Information

You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: [1-866-653-4261](tel:1-866-653-4261). The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General. This notice has not been delayed by law enforcement.

For New York residents, the New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; [1-800-771-7755](tel:1-800-771-7755); or <https://ag.ny.gov/>.

For North Carolina residents, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; [1-877-566-7226](tel:1-877-566-7226) or [1-919-716-6000](tel:1-919-716-6000); and www.ncdoj.gov.

EXHIBIT 2



AR
HEALTH

PATIENT RIGHTS AND RESPONSIBILITIES

Policy:

This Center does not discriminate on the basis of sex, race, age, political affiliations, disability, national origin, language, sexual orientation, gender identity, or religious preference in the consideration of any patient.

STATEMENT

Providing Information:

Patients/families are responsible for providing the most accurate and complete information concerning their condition including past medical history and services received from other health care providers.

Access to Information:

The patient has the right to obtain complete and current information regarding his/her diagnosis and treatment unless it is determined to be medically inadvisable to give such information. In this case, the information will be made available to an appropriate person on the patient's behalf. The patient has the right to examine and receive an explanation of his bill regardless of the source of payment, the patient and family will help the organization improve its understanding of patient needs and expectations by providing feedback concerning clinic services.

Treatment Consent/Refusal:

The patient has the right to receive information necessary to give informed consent prior to the start of any procedure or treatment. This includes providing information on medically significant alternative care or treatment (when it exists). Patients have the right to appropriate assessment and management of pain.

Patients/families are responsible for following the plan of care and setting self-management goals; expressing concerns regarding their ability to comply; and understanding the consequences of not complying, being responsible for the outcomes when not following the plan of care. If a patient does not understand proposed care, he/she is responsible for making this known. The patient has the right to select a primary care provider and request a second opinion or refuse treatment to the extent permitted by law. Patients will be provided with information about Advance Directives and assistance when requested.

Confidentiality:

The patient has the right to every consideration of privacy concerning medical records. All records and communications pertaining to medical care will be confidential. Those not directly involved in the patient care must have the permission of the patient to be present.

Continuity of Care:

The patient has the right to expect a reasonable response from the clinic to requests for services. Primary Health is responsible for coordinating patient care across multiple care settings and will provide services or referrals as indicated by the urgency of the case. The patient has the responsibility to comply with follow-up care and appointments as prescribed by the provider.

Rules:

Patients and family must follow the organization's rules and regulations governing patient care and conduct. Patients are responsible for co-pays for services rendered as well as charges not paid or denied by insurance.

Respect and Consideration:

The patient has the right to considerate and respectful care. Patients and family must show consideration to other patients and staff as well as respecting the property of others and of the organization.

EXHIBIT 1

26442

ARcare
P.O. Box 989728
West Sacramento, CA 95798-9728

To Enroll, Please Call:
(833) 783-1354
Or Visit:
<https://response.idx.us/arcare>
Enrollment Code: <<ENROLLMENT>>

<<Full Name>>
<<ADDRESS1>>
<<ADDRESS2>>
<<CITY>>, <<STATE>> <<ZIP>>

April 25, 2022

<<HEADER>>

Dear <<Full Name>>:

ARcare writes to inform you of a recent incident that may affect the privacy of some of your information. Although ARcare is unaware of any actual or attempted misuse of your information, ARcare is providing you notice of the incident, steps ARcare is taking in response, and resources available to help you better protect your information, should you feel it is appropriate to do so.

What Happened? On February 24, 2022, ARcare learned of a data security incident affecting its systems. ARcare immediately worked to secure its systems and quickly commenced an investigation to confirm the nature and scope of the incident. Through that investigation, ARcare determined that your information was in files that a third party may have accessed or acquired without authorization.

What Information Was Involved? As indicated above, ARcare is unaware of any actual misuse of your personal information. However, the information present in the files that were accessed and/or acquired as a result of the incident may have included your <<Variable Text 2>>, and name.

What We Are Doing. ARcare treats its responsibility to safeguard information in its care as an utmost priority. As such, ARcare responded immediately to this incident and has worked diligently to provide you with an accurate and complete notice of the incident as soon as possible. As part of its ongoing commitment to the privacy and security of personal information in its care, ARcare is reviewing and updating existing policies and procedures relating to data protection and security. ARcare is also investigating additional security measures to mitigate any risk associated with this incident and to better prevent future similar incidents. ARcare is providing notice of this incident to potentially impacted individuals and to regulators where required.

Out of an abundance of caution, ARcare is providing you with <<CM Length>> months of complimentary access to credit and CyberScan monitoring, a \$1,000,000 insurance reimbursement policy, and fully managed identity theft recovery services through IDX, as well as guidance on how to better protect your information, should you feel it is appropriate to do so. Although ARcare is covering the cost of these services, due to privacy restrictions, you will need to complete the activation process yourself. Please note the deadline for enrollment is July 25, 2022.

Incident Timeline. After learning of the data security incident, ARcare quickly commenced an investigation with the assistance of third-party cybersecurity specialists. On or about March 14, 2022, the investigation determined that an unauthorized actor accessed and/or acquired data from ARcare's systems between January 18, 2022 and February 24, 2022. A thorough review of the contents of the affected data was subsequently performed to determine whether it contained any sensitive information and identify affected individuals. On or about April 4, 2022, ARcare concluded the review and determined that your information may have been affected as a result of the incident.

What You Can Do. Although there is no evidence of any actual or attempted misuse of your information, ARcare encourages you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements, explanation of benefits, and monitoring your free credit reports for suspicious activity and to detect errors over the next 12 to 24 months. Any suspicious activity should be reported to the appropriate insurance company, health care provider, or financial institution. You can also find out more about how to safeguard your information in the enclosed *Steps You Can Take to Protect Personal Information*. There, you will find additional information about the complimentary credit monitoring services and how to enroll.

For More Information. We understand you may have questions about this incident that are not addressed in this letter. To ensure your questions are answered in a timely manner, please call our dedicated assistance line at: (833) 783-1354, available Monday through Friday from 8 am - 8 pm Central Time. You may also write to us directly at: 117 S. 2nd Street, Augusta, Arkansas 72006.

ARcare apologizes for any inconvenience this incident may cause you. ARcare remains committed to privacy and security of information in its possession.

Steps You Can Take to Protect Personal Information

Enroll in Complimentary Credit Monitoring

1. **Website and Enrollment.** Go to <https://response.idx.us/arcare> and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter.
2. **Activate the credit monitoring** provided as part of your IDX identity protection membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, IDX will be able to assist you.
3. **Telephone.** Contact IDX at (833) 783-1354 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

Monitor Your Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also directly contact the three major credit reporting bureaus listed below to request a free copy of your credit report.

Consumers have the right to place an initial or extended “fraud alert” on a credit file at no cost. An initial fraud alert is a one-year alert that is placed on a consumer’s credit file. Upon seeing a fraud alert display on a consumer’s credit file, a business is required to take steps to verify the consumer’s identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a “credit freeze” on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer’s express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a credit freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. To request a credit freeze, you will need to provide the following information:

1. Full name (including middle initial, as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver’s license or ID card, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if you are a victim of identity theft.

Should you wish to place a fraud alert or a credit freeze, please contact the three major credit reporting bureaus listed below:

Equifax	Experian	TransUnion
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
1-888-298-0045	1-888-397-3742	1-833-395-6938
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Additional Information

You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General. This notice has not been delayed by law enforcement.

For New York residents, the New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or <https://ag.ny.gov/>.

For North Carolina residents, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.

JS 44 (Rev. 04/21)

CIVIL COVER SHEET *4:22cv454-KGB*

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.)

<p>I. (a) PLAINTIFFS Jessica White</p> <p>(b) County of Residence of First Listed Plaintiff <u>Pulaski County</u> (EXCEPT IN U.S. PLAINTIFF CASES)</p> <p>(c) Attorneys (Firm Name, Address, and Telephone Number) Christopher D. Jennings- JOHNSON FIRM 610 President Clinton Avenue, Suite 300 Little Rock, Arkansas 72201 Telephone: (501) 372-1300</p>	<p>DEFENDANTS ARcare</p> <p>County of Residence of First Listed Defendant <u>Woodruff County</u> (IN U.S. PLAINTIFF CASES ONLY)</p> <p>NOTE: IN LAND CONDEMNATION CASES, USE THE LOCATION OF THE TRACT OF LAND INVOLVED.</p> <p>Attorneys (If Known)</p>
--	---

<p>II. BASIS OF JURISDICTION (Place an "X" in One Box Only)</p> <p><input type="checkbox"/> 1 U.S. Government Plaintiff</p> <p><input type="checkbox"/> 2 U.S. Government Defendant</p> <p><input type="checkbox"/> 3 Federal Question (U.S. Government Not a Party)</p> <p><input checked="" type="checkbox"/> 4 Diversity (Indicate Citizenship of Parties in Item III)</p>	<p>III. CITIZENSHIP OF PRINCIPAL PARTIES (Place an "X" in One Box for Plaintiff and One Box for Defendant)</p> <table style="width:100%;"> <tr> <td style="width:33%;">Citizen of This State</td> <td style="width:33%;">Incorporated or Principal Place of Business In This State</td> <td style="width:33%;">PTF DEF</td> </tr> <tr> <td><input type="checkbox"/> 1</td> <td><input type="checkbox"/> 1</td> <td><input type="checkbox"/> 4 <input checked="" type="checkbox"/> 4</td> </tr> <tr> <td>Citizen of Another State</td> <td>Incorporated and Principal Place of Business In Another State</td> <td></td> </tr> <tr> <td><input checked="" type="checkbox"/> 2</td> <td><input type="checkbox"/> 2</td> <td><input type="checkbox"/> 5 <input type="checkbox"/> 5</td> </tr> <tr> <td>Citizen or Subject of a Foreign Country</td> <td>Foreign Nation</td> <td></td> </tr> <tr> <td><input type="checkbox"/> 3</td> <td><input type="checkbox"/> 3</td> <td><input type="checkbox"/> 6 <input type="checkbox"/> 6</td> </tr> </table>	Citizen of This State	Incorporated or Principal Place of Business In This State	PTF DEF	<input type="checkbox"/> 1	<input type="checkbox"/> 1	<input type="checkbox"/> 4 <input checked="" type="checkbox"/> 4	Citizen of Another State	Incorporated and Principal Place of Business In Another State		<input checked="" type="checkbox"/> 2	<input type="checkbox"/> 2	<input type="checkbox"/> 5 <input type="checkbox"/> 5	Citizen or Subject of a Foreign Country	Foreign Nation		<input type="checkbox"/> 3	<input type="checkbox"/> 3	<input type="checkbox"/> 6 <input type="checkbox"/> 6
Citizen of This State	Incorporated or Principal Place of Business In This State	PTF DEF																	
<input type="checkbox"/> 1	<input type="checkbox"/> 1	<input type="checkbox"/> 4 <input checked="" type="checkbox"/> 4																	
Citizen of Another State	Incorporated and Principal Place of Business In Another State																		
<input checked="" type="checkbox"/> 2	<input type="checkbox"/> 2	<input type="checkbox"/> 5 <input type="checkbox"/> 5																	
Citizen or Subject of a Foreign Country	Foreign Nation																		
<input type="checkbox"/> 3	<input type="checkbox"/> 3	<input type="checkbox"/> 6 <input type="checkbox"/> 6																	

IV. NATURE OF SUIT (Place an "X" in One Box Only) Click here for: Nature of Suit Code Descriptions.

CONTRACT	TORTS	FORFEITURE/PENALTY	BANKRUPTCY	OTHER STATUTES	
<input type="checkbox"/> 110 Insurance <input type="checkbox"/> 120 Marine <input type="checkbox"/> 130 Miller Act <input type="checkbox"/> 140 Negotiable Instrument <input type="checkbox"/> 150 Recovery of Overpayment & Enforcement of Judgment <input type="checkbox"/> 151 Medicare Act <input type="checkbox"/> 152 Recovery of Defaulted Student Loans (Excludes Veterans) <input type="checkbox"/> 153 Recovery of Overpayment of Veteran's Benefits <input type="checkbox"/> 160 Stockholders' Suits <input type="checkbox"/> 190 Other Contract <input type="checkbox"/> 195 Contract Product Liability <input type="checkbox"/> 196 Franchise	<p>PERSONAL INJURY</p> <input type="checkbox"/> 310 Airplane <input type="checkbox"/> 315 Airplane Product Liability <input type="checkbox"/> 320 Assault, Libel & Slander <input type="checkbox"/> 330 Federal Employers' Liability <input type="checkbox"/> 340 Marine <input type="checkbox"/> 345 Marine Product Liability <input type="checkbox"/> 350 Motor Vehicle <input type="checkbox"/> 355 Motor Vehicle Product Liability <input type="checkbox"/> 360 Other Personal Injury <input type="checkbox"/> 362 Personal Injury - Medical Malpractice	<p>PERSONAL INJURY</p> <input type="checkbox"/> 365 Personal Injury - Product Liability <input type="checkbox"/> 367 Health Care/Pharmaceutical Personal Injury Product Liability <input type="checkbox"/> 368 Asbestos Personal Injury Product Liability <p>PERSONAL PROPERTY</p> <input type="checkbox"/> 370 Other Fraud <input type="checkbox"/> 371 Truth in Lending <input checked="" type="checkbox"/> 380 Other Personal Property Damage <input type="checkbox"/> 385 Property Damage Product Liability	<input type="checkbox"/> 625 Drug Related Seizure of Property 21 USC 881 <input type="checkbox"/> 690 Other	<input type="checkbox"/> 422 Appeal 28 USC 158 <input type="checkbox"/> 423 Withdrawal 28 USC 157 <p>INTELLECTUAL PROPERTY RIGHTS</p> <input type="checkbox"/> 820 Copyrights <input type="checkbox"/> 830 Patent <input type="checkbox"/> 835 Patent - Abbreviated New Drug Application <input type="checkbox"/> 840 Trademark <input type="checkbox"/> 880 Defend Trade Secrets Act of 2016 <p>SOCIAL SECURITY</p> <input type="checkbox"/> 861 HIA (1395ff) <input type="checkbox"/> 862 Black Lung (923) <input type="checkbox"/> 863 DIWC/DIWW (405(g)) <input type="checkbox"/> 864 SSID Title XVI <input type="checkbox"/> 865 RSI (405(g)) <p>FEDERAL TAX SUITS</p> <input type="checkbox"/> 870 Taxes (U.S. Plaintiff or Defendant) <input type="checkbox"/> 871 IRS—Third Party 26 USC 7609	<input type="checkbox"/> 375 False Claims Act <input type="checkbox"/> 376 Qui Tam (31 USC 3729(a)) <input type="checkbox"/> 400 State Reapportionment <input type="checkbox"/> 410 Antitrust <input type="checkbox"/> 430 Banks and Banking <input type="checkbox"/> 450 Commerce <input type="checkbox"/> 460 Deportation <input type="checkbox"/> 470 Racketeer Influenced and Corrupt Organizations <input type="checkbox"/> 480 Consumer Credit (15 USC 1681 or 1692) <input type="checkbox"/> 485 Telephone Consumer Protection Act <input type="checkbox"/> 490 Cable/Sat TV <input type="checkbox"/> 850 Securities/Commodities/Exchange <input type="checkbox"/> 890 Other Statutory Actions <input type="checkbox"/> 891 Agricultural Acts <input type="checkbox"/> 893 Environmental Matters <input type="checkbox"/> 895 Freedom of Information Act <input type="checkbox"/> 896 Arbitration <input type="checkbox"/> 899 Administrative Procedure Act/Review or Appeal of Agency Decision <input type="checkbox"/> 950 Constitutionality of State Statutes
<p>REAL PROPERTY</p> <input type="checkbox"/> 210 Land Condemnation <input type="checkbox"/> 220 Foreclosure <input type="checkbox"/> 230 Rent Lease & Ejectment <input type="checkbox"/> 240 Torts to Land <input type="checkbox"/> 245 Tort Product Liability <input type="checkbox"/> 290 All Other Real Property	<p>CIVIL RIGHTS</p> <input type="checkbox"/> 440 Other Civil Rights <input type="checkbox"/> 441 Voting <input type="checkbox"/> 442 Employment <input type="checkbox"/> 443 Housing/Accommodations <input type="checkbox"/> 445 Amer. w/Disabilities - Employment <input type="checkbox"/> 446 Amer. w/Disabilities - Other <input type="checkbox"/> 448 Education	<p>PRISONER PETITIONS</p> <p>Habeas Corpus:</p> <input type="checkbox"/> 463 Alien Detainee <input type="checkbox"/> 510 Motions to Vacate Sentence <input type="checkbox"/> 530 General <input type="checkbox"/> 535 Death Penalty <p>Other:</p> <input type="checkbox"/> 540 Mandamus & Other <input type="checkbox"/> 550 Civil Rights <input type="checkbox"/> 555 Prison Condition <input type="checkbox"/> 560 Civil Detainee - Conditions of Confinement	<input type="checkbox"/> 710 Fair Labor Standards Act <input type="checkbox"/> 720 Labor/Management Relations <input type="checkbox"/> 740 Railway Labor Act <input type="checkbox"/> 751 Family and Medical Leave Act <input type="checkbox"/> 790 Other Labor Litigation <input type="checkbox"/> 791 Employee Retirement Income Security Act <p>IMMIGRATION</p> <input type="checkbox"/> 462 Naturalization Application <input type="checkbox"/> 465 Other Immigration Actions		

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:
Negligence, Breach of Implied Contract, Invasion of Privacy, Breach of Confidence

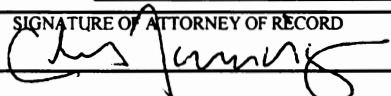
VII. REQUESTED IN COMPLAINT:

CHECK IF THIS IS A CLASS ACTION UNDER RULE 23, F.R.Cv.P. **DEMAND \$** _____ CHECK YES only if demanded in complaint:
JURY DEMAND: Yes No

VIII. RELATED CASE(S) IF ANY (See instructions):

JUDGE _____ DOCKET NUMBER _____

DATE May 16, 2022

SIGNATURE OF ATTORNEY OF RECORD 

FOR OFFICE USE ONLY

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

ClassAction.org

This complaint is part of ClassAction.org's searchable [class action lawsuit database](#)
