

FILED
U.S. DISTRICT COURT
EASTERN DISTRICT ARKANSAS

JUN 17 2022

**UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF ARKANSAS**

TAMMY H. DOWNS, CLERK
By: *Kittelyn* DEP CLERK

MELISSA JOHNSON, individually and on behalf of all others similarly situated,

Plaintiff,

v.

ARCARE,

Defendant.

Case No. 4:22-cv-571-BSM

JURY TRIAL DEMANDED

This case assigned to District Judge Miller
and to Magistrate Judge Ervin

Plaintiff Melissa Johnson (“Plaintiff” or “Ms. Johnson”) brings this Class Action Complaint against ARcare (“Defendant” or “ARcare”), individually and on behalf of all others similarly situated (“Class Members”), and alleges, upon personal knowledge as to her own actions and her counsel’s 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 including, but not limited to, names, dates of birth and Social Security numbers (collectively, “personally identifiable information” or “PII”) and medical diagnosis or condition information and health insurance information (“protected health information” or “PHI”).

2. According to Defendant's website, Defendant is a healthcare network throughout Arkansas, Kentucky and Mississippi.¹

3. On February 24, 2022, Defendant experienced a data security incident that

¹ <https://www.arcare.net/our-story/> (last visited Apr. 26, 2022).

impacted its computer systems and caused a temporary disruption to services (the “Data Breach”).²

4. Defendant immediately worked to secure its systems and quickly commenced an investigation to confirm the nature and scope of the incident.³

5. On March 14, 2022, the investigation determined that an unauthorized actor may have accessed and/or acquired sensitive data during a period of unauthorized access to Defendant’s computer systems between January 18 and February 24, 2022.⁴

6. A review of the contents of the affected data was subsequently performed to determine whether it contained any sensitive information and identify affected individuals.⁵

7. On April 4, 2022, Defendant concluded the review and determined that at least the following sensitive information was compromised: “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.”⁶

8. The investigation determined that an unauthorized actor gained access to Defendant’s systems and that information contained in those systems was, in all likelihood, viewed and/or taken by the unauthorized actor.⁷

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

² <https://www.arcare.net/wp-content/uploads/2022/04/ARcare-Security-Notice.pdf> (last visited May 3, 2022).

³ *Id.*

⁴ *Id.*

⁵ *Id.*

⁶ *Id.*

⁷ *Id.*

to protect and safeguard that information from unauthorized access and intrusion. Defendant admits that the unencrypted PII and PHI impacted during the Data Breach included 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.

10. The exposed PII and PHI of Plaintiff and Class Members can—and likely will—be sold on the dark web. Hackers can offer for sale the unencrypted, unredacted PII and PHI to criminals. Plaintiff and Class Members now face a lifetime risk of identity theft, which is heightened here by the loss of Social Security numbers - the gold standard for identity thieves.

11. This PII and PHI was 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. In addition to Defendant's failure to prevent the Data Breach, after discovering the Breach, Defendant waited several months to report it to government agencies and affected individuals.

12. As a result of this delayed response, Plaintiff and Class Members had no idea their PII and PHI had been compromised, and that they were, and continue to be, at significant risk of identity theft and various other forms of personal, social, and financial harm. The risk will remain for their respective lifetimes.

13. Plaintiff brings this action on behalf of all persons whose PII and PHI was 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 Defendant's inadequate information security practices; and (iii) effectively secure hardware containing protected PII and PHI using reasonable and effective security procedures free of vulnerabilities and incidents.

Defendant's conduct amounts to negligence and violates federal and state statutes.

14. 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 time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time, and (iv) the continued and substantially 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.

15. Defendant disregarded the rights of Plaintiff and Class Members by intentionally, willfully, recklessly, and/or negligently failing to take and implement adequate and reasonable measures to ensure that the PII and PHI of Plaintiff and Class Members 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 compromised through disclosure to 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

16. Plaintiff Melissa Johnson is a citizen of Blytheville, residing in Mississippi

County.

17. Defendant ARcare is a corporation organized under the laws of Arkansas, headquartered at 117 South 2nd Street in Augusta, with its principal place of business in Augusta, Arkansas.

18. 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.

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

III. JURISDICTION AND VENUE

20. This Court has jurisdiction under the Class Action Fairness Act ("CAFA"), 28 U.S.C. § 1332(d), because: "(1) there is minimal diversity; (2) the proposed class contains at least 100 members; and (3) the amount in controversy is at least \$5 million in the aggregate." *Raskas v. Johnson & Johnson*, 719 F.3d 884, 886 (8th Cir. 2013) (quoting *Plubell v. Merck & Co.*, 434 F.3d 1070, 1071 (8th Cir. 2006)).

21. 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 conducts substantial business in Arkansas and this District through its headquarters, offices, parents, and affiliates.

22. 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.

23. Plaintiff and Class Members directly or indirectly entrusted Defendant with sensitive and confidential information, including their PII and PHI, which includes information that is static, does not change, and can be used to commit myriad financial crimes.

24. Plaintiff and Class Members 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. Plaintiff and Class Members demand Defendant safeguard their PII and PHI.

25. Defendant had a duty to adopt reasonable measures to protect the PII and PHI of Plaintiff and Class Members from involuntary disclosure to third parties.

26. Defendant's privacy notice states:

COMMITMENT TO YOUR PRIVACY

Our 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). In conducting our business, we will create records regarding you and the treatment and services we provide to you. We are required by law to maintain the confidentiality of information that identifies you. We also are required by law to provide you with this notice of our legal duties and the privacy practices that we maintain in our practice concerning your Personally Identifiable Information (PII). By federal and state law, we must follow the terms of the notice of privacy practices that we have in effect at the time.⁸

27. On April 25, 2022, Defendant notified the United States Department of Health and Human Services of the Data Breach ("Notice of Data Breach").⁹ Defendant advised that the

⁸ <https://www.arcare.net/privacy-statement/> (last visited May 3, 2022).

⁹ https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (last visited May 3, 2022).

information potentially impacted in the Data Breach, included names, addresses, dates of birth, Social Security numbers, driver's licenses, Passports, financial account information, payment card information, employer-assigned identification number, medical information, and biometric data.

28. The Notice of Data Breach stated, in relevant part, the following:

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 ARcare's 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, 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. 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.¹⁰

29. Defendant admitted in the Notice of Data Breach that unauthorized third persons accessed files that contained Plaintiff's and Class's Members' PII and PHI.

30. The unencrypted PII and PHI of Plaintiff and Class Members will likely end up for sale on the dark web as that is the *modus operandi* of hackers. In addition, unencrypted PII and PHI may fall into the hands of companies that will use the detailed PII and PHI for targeted marketing without the approval of Plaintiff and Class Members. In turn, unauthorized individuals can easily access the PII and PHI of Plaintiff and Class Members.

31. Defendant did not use reasonable security procedures and practices appropriate to the nature of the sensitive, unencrypted information they were maintaining for Plaintiff and Class Members, causing the exposure of PII and PHI.

32. As explained by the Federal Bureau of Investigation, “[p]revention is the most effective defense against ransomware and it is critical to take precautions for protection.”¹¹

33. To prevent and detect unauthorized cyber-attacks, Defendant could and should have implemented, as recommended by the United States Government, the following measures:

- Implement an awareness and training program. Because end users are targets, employees and individuals should be aware of the threat of ransomware and how it is delivered.
- Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.
- Scan all incoming and outgoing emails to detect threats and filter executable files

¹⁰ See *supra*, Fn. 2.

¹¹ See How to Protect Your Networks from RANSOMWARE, at 3, available at <https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view> (last visited Aug. 23, 2021).

from reaching end users.

- Configure firewalls to block access to known malicious IP addresses.
- Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system.
- Set anti-virus and anti-malware programs to conduct regular scans automatically.
- Manage the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.
- Configure access controls-including file, directory, and network share permissions-with least privilege in mind. If a user only needs to read specific files, the user should not have write access to those files, directories, or shares.
- Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.
- Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.
- Consider disabling Remote Desktop protocol (RDP) if it is not being used.
- Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.
- Execute operating system environments or specific programs in a virtualized environment.
- Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.¹²

34. To prevent and detect cyber-attacks, including the cyber-attack that resulted in the Data Breach, Defendant could and should have implemented, as recommended by the United States Cybersecurity & Infrastructure Security Agency, the following measures:

¹² *Id.* at 3-4.

- **Update and patch your computer.** Ensure your applications and operating systems (OSs) have been updated with the latest patches. Vulnerable applications and OSs are the target of most ransomware attacks....
- **Use caution with links and when entering website addresses.** Be careful when clicking directly on links in emails, even if the sender appears to be someone you know. Attempt to independently verify website addresses (e.g., contact your organization's helpdesk, search the internet for the sender organization's website or the topic mentioned in the email). Pay attention to the website addresses you click on, as well as those you enter yourself. Malicious website addresses often appear almost identical to legitimate sites, often using a slight variation in spelling or a different domain (e.g., .com instead of .net)....
- **Open email attachments with caution.** Be wary of opening email attachments, even from senders you think you know, particularly when attachments are compressed files or ZIP files.
- **Keep your personal information safe.** Check a website's security to ensure the information you submit is encrypted before you provide it....
- **Verify email senders.** If you are unsure whether or not an email is legitimate, try to verify the email's legitimacy by contacting the sender directly. Do not click on any links in the email. If possible, use a previous (legitimate) email to ensure the contact information you have for the sender is authentic before you contact them.
- **Inform yourself.** Keep yourself informed about recent cybersecurity threats and up to date on ransomware techniques. You can find information about known phishing attacks on the Anti-Phishing Working Group website. You may also want to sign up for CISA product notifications, which will alert you when a new Alert, Analysis Report, Bulletin, Current Activity, or Tip has been published.
- **Use and maintain preventative software programs.** Install antivirus software, firewalls, and email filters-and keep them updated-to reduce malicious network traffic.¹³

35. To prevent and detect cyber-attacks, including the cyber-attack that resulted in the Data Breach, Defendant could and should have implemented, as recommended by the Microsoft Threat Protection Intelligence Team, the following measures:

Secure internet-facing assets

¹³ See Security Tip (STI 9-001) Protecting Against Ransomware (original release date Apr. 11, 2019), available at <https://us-cert.cisa.gov/ncas/tips/ST19-001> (last visited Aug. 23, 2021).

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

Thoroughly investigate and remediate alerts

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

Include IT Pros in security discussions

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

Build credential hygiene

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

Apply principle of least-privilege

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

Harden infrastructure

- Use Windows Defender Firewall
- Enable tamper protection
- Enable cloud-delivered protection
- Turn on attack surface reduction rules and [Antimalware Scan Interface] for Office [Visual Basic for Applications].¹⁴

36. Given that Defendant was storing the PII and PHI of Plaintiff and Class Members, Defendant could and should have implemented all of the above measures to prevent and detect

¹⁴ See Human-operated ransomware attacks: A preventable disaster (Mar. 5, 2020), *available at* <https://microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/> (last visited Aug. 23, 2021).

cyberattacks.

37. The occurrence of the Data Breach indicates that Defendant failed to adequately implement one or more of the above measures to prevent cyberattacks, resulting in the Data Breach and the exposure of the PII and PHI of Plaintiff and Class Members.

Defendant Acquires, Collects, and Stores the PII and PHI of Plaintiff and Class Members.

38. Defendant acquired, collected, and stored the PII and PHI of Plaintiff and Class Members.

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 PHI and Preventing Breaches

41. Defendant could have prevented this Data Breach by properly securing and encrypting the systems containing the PII and PHI of Plaintiff and Class Members. Alternatively, Defendant could have destroyed the data, especially for individuals with whom it had not had a relationship for a period of time.

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

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.”¹⁵ 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.”¹⁶

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

Value of PII and PHI

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 \$200.¹⁷ Experian reports that a stolen credit or debit card number can sell for \$5 to \$110 on the dark web.¹⁸ Criminals can also purchase access

¹⁵ 17 C.F.R. §248.201 (2013).

¹⁶ *Id.*

¹⁷ *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 accessed Oct. 27, 2021).

¹⁸ *Here’s How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec.

to entire company data breaches from \$900 to \$4,500.¹⁹

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 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.²⁰

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, "[t]he credit bureaus and banks are able to link

6, 2017, available at <https://www.experian.com/blohs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/> (last accessed Oct. 27, 2021).

¹⁹ *In the Dark*, VPNOverview, 2019, available at: <https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/> (last accessed Oct. 27, 2021).

²⁰ Social Security Administration, *Identity Theft and Your Social Security Number*, available at: <https://www.ssa.gov/pubs/EN-05-10064.pdf> (last accessed Oct. 27, 2021).

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.”²¹

50. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach because, there, victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach is impossible to “close” and difficult, if not impossible, to change—Social Security number and name.

51. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, “[c]ompared to credit card information, personally identifiable information and Social Security numbers are worth more than 10x on the black market.”²²

52. 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.

53. The fraudulent activity resulting from the Data Breach may not come to light for years.

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

²¹ 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 accessed Oct. 27, 2021).

²² Tim 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 accessed Aug. 23, 2021).

55. 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.

56. According to account monitoring company LogDog, medical data, such as PHI, sells for \$50 and up on the Dark Web.²³

57. Moreover, there may be a time lag between when harm occurs versus when it is discovered, and also between when PII 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.²⁴

58. 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 of the foreseeable consequences that would occur if Defendant's data security system was breached, including, specifically, the significant costs that would be imposed on Plaintiff and Class Members as a result of a breach.

59. Plaintiff and Class Members now face years of constant surveillance of their

²³ Lisa Vaas, *Ransomware Attacks Paralyze, and Sometimes Crush, Hospitals*, Naked Security (Oct. 3, 2019), <https://nakedsecurity.sophos.com/2019/10/03/ransomware-attacks-paralyze-and-sometimes-crush-hospitals/#content> (last accessed July 20, 2021).

²⁴ *Report to Congressional Requesters*, GAO, at 29 (June 2007), available at: <https://www.gao.gov/assets/gao-07-737.pdf> (last accessed Aug. 23, 2021).

financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their PII and PHI.

60. Defendant was, or should have been, fully aware of the unique type and the significant volume of data on Defendant's network, amounting to potentially millions of individuals' detailed, personal information and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

61. To date, Defendant has offered Plaintiff and Class Members only 12 months of identity and credit monitoring services through Experian. 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. Moreover, Defendant put the burden squarely on Plaintiff and Class Members to enroll in the inadequate monitoring services.

62. 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.

Plaintiff's Experience

63. Plaintiff entrusted her PII and PHI to Defendant.

64. At the time of the Data Breach, Defendant retained Plaintiff's name, date of birth, Social Security number, medical treatment information, prescription information, medical diagnoses/condition information, and health insurance information.

65. Plaintiff received Defendant's Notice of Data Breach in early May of 2022.

66. The Notice stated that Plaintiff's PII and PHI was among the information accessed or acquired during the Data Breach.

67. Plaintiff diligently monitors her credit score and noticed her credit score dropped

dramatically following the Data Breach.

68. Plaintiff reviewed her credit report and found multiple fraudulent accounts that unauthorized individuals had attempted to open in her name. These accounts were opened in states such as New York and Texas, where Plaintiff has never resided.

69. There was also an unauthorized account opened related to Plaintiff's medical records.

70. Plaintiff has begun to dispute the fraudulent accounts.

71. Plaintiff has spent over twenty (20) hours responding to the Data Breach.

72. As a result of the Data Breach notice, Plaintiff spent time dealing with the consequences of the Data Breach, which includes time spent verifying the legitimacy of the Notice of Data Breach, self-monitoring her accounts and credit reports to ensure no further fraudulent activity has occurred. This time has been lost forever and cannot be recaptured. Moreover, this time was spent at Defendant's direction by way of the Data Breach notice where Defendant advised Plaintiff to mitigate her damages by, among other things, monitoring her accounts for fraudulent activity.

73. Plaintiff is very careful about sharing her sensitive PII and PHI. Plaintiff has never knowingly transmitted unencrypted sensitive PII and PHI over the internet or any other unsecured source.

74. Plaintiff stores any documents containing her sensitive PII and PHI in a safe and secure location or destroys the documents. Moreover, Plaintiff diligently chooses unique usernames and passwords for her various online accounts.

75. Plaintiff suffered actual injury in the form of damages to and diminution in the value of Plaintiff's PII and PHI—a form of intangible property that Plaintiff entrusted to

Defendant, which was compromised in and as a result of the Data Breach. 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.

76. Plaintiff has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from her PII and PHI being placed in the hands of unauthorized third parties and possibly criminals.

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

V. CLASS ALLEGATIONS

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

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

All United States residents whose PII and PHI was actually or potentially accessed or acquired during the Data Breach event that is the subject of the Notice of Data Breach that Defendant published to Plaintiff and other Class Members on or around April 22, 2022 (the "Nationwide Class").

80. Excluded from the Class 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.

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

82. Numerosity, Fed. R. Civ. P. 23(a)(1): The Nationwide Class members are so numerous that joinder of all members is impracticable. Upon information and belief, there are hundreds, if not thousands, of individuals whose PII and PHI may have been improperly accessed in the Data Breach, and each Class is apparently identifiable within Defendant's records.

83. Commonality, Fed. R. Civ. P. 23(a)(2) and (b)(3): Questions of law and fact common to the Classes exist and predominate over any questions affecting only individual Class Members. These include:

- 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 duties not to disclose the PII and PHI of Plaintiff and Class Members to unauthorized third parties;
- c. Whether Defendant had duties 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;
- 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 compromised;
- g. Whether Defendant violated the law by failing to promptly notify Plaintiff

and Class Members that their PII and PHI had been 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 that permitted the Data Breach to occur;
- j. Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard the PII and PHI of Plaintiff and Class Members;
- k. Whether Defendant violated the consumer protection statutes invoked herein;
- l. Whether Plaintiff and Class Members are entitled to actual, consequential, and/or nominal damages as a result of Defendant's wrongful conduct;
- m. Whether Defendant knowingly made false representations as to its data security practices;
- n. Whether Plaintiff and Class Members are entitled to restitution as a result of Defendant's wrongful conduct; and
- o. 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.

78. Typicality, Fed. R. Civ. P. 23(a)(3): Plaintiff's claims are typical of those of other Class Members because all had their PII and PHI compromised as a result of the Data Breach, due to Defendant's misfeasance.

79. Policies Generally Applicable to the Class: This class action is also appropriate

for certification because Defendant has acted or refused to act on grounds generally applicable to the Class, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members and making final injunctive relief appropriate with respect to the Class as a whole. Defendant's policies challenged herein apply to and affect Class Members uniformly and Plaintiff's challenge of these policies hinges on Defendant's conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiff.

80. Adequacy, Fed. R. Civ. P. 23(a)(4): Plaintiff will fairly and adequately represent and protect the interests of the Class Members in that Plaintiff has no disabling conflicts of interest that would be antagonistic to those of the other Members of the Class. Plaintiff seeks no relief that is antagonistic or adverse to the Members of the Class and the infringement of the rights and the damages Plaintiff has suffered are typical of other Class Members. Plaintiff has also retained counsel experienced in complex class action litigation, and Plaintiff intends to prosecute this action vigorously.

81. Superiority and Manageability, Fed. R. Civ. P. 23(b)(3): Class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of Class Members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain Class Members, who could not individually afford to litigate a complex claim against large corporations, like Defendant. Further, even for those Class Members who could afford to litigate such a claim,

it would still be economically impractical and impose a burden on the courts.

82. The nature of this action and the nature of laws available to Plaintiff and Class Members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiff and Class Members for the wrongs alleged because Defendant would necessarily gain an unconscionable advantage since they would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiff were exposed is representative of that experienced by the Class and will establish the right of each Class Member to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

83. The litigation of the claims brought herein is manageable. Defendant's uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrates that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

84. Adequate notice can be given to Class Members directly using information maintained in Defendant's records.

85. Unless a Class-wide injunction is issued, Defendant may continue in its failure to properly secure the PII and PHI of Class Members, Defendant may continue to refuse to provide proper notification to Class Members regarding the Data Breach, and Defendant may continue to act unlawfully as set forth in this Complaint.

86. Further, Defendant has acted or refused to act on grounds generally applicable to the Classes and, accordingly, final injunctive or corresponding declaratory relief with regard to

the Class Members as a whole is appropriate under Rule 23(b)(2) of the Federal Rules of Civil Procedure.

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

- a. Whether Defendant owed a legal duty to Plaintiff and Class Members to exercise due care in collecting, storing, using, and safeguarding their PII and PHI;
- b. Whether Defendant breached a legal duty to Plaintiff and Class Members to exercise due care in collecting, storing, using, and safeguarding their PII and PHI;
- c. Whether Defendant failed to comply with its own policies and applicable laws, regulations, and industry standards relating to data security;
- d. Whether an implied contract existed between Defendant on the one hand, and Plaintiff and Class Members on the other, and the terms of that implied contract;
- e. Whether Defendant breached the implied contract;
- f. Whether Defendant adequately and accurately informed Plaintiff and Class Members that their PII and PHI had been compromised;
- g. 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;

- h. Whether Class Members are entitled to actual, consequential, and/or nominal damages, and/or injunctive relief as a result of Defendant's wrongful conduct.

VI. CAUSES OF ACTION

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

88. Plaintiff and the Class repeat and re-allege each and every allegation in the Complaint as if fully set forth herein.

89. Plaintiff and the Class entrusted Defendant with their PII and/or PHI.

90. Plaintiff and the Class entrusted their PII and/or PHI to Defendant on the premise and with the understanding that Defendant would safeguard their information, use their PII and/or PHI for business purposes only, and/or not disclose their PII and/or PHI to unauthorized third parties.

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

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

93. 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 Classes in Defendant's possession was adequately secured and protected.

94. Defendant also had a duty to exercise appropriate clearinghouse practices to remove PII and/or PHI they were no longer required to retain pursuant to regulations.

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

96. Defendant's duty to use reasonable security measures arose as a result of the special relationship that existed between Defendant and Plaintiff and the Class. That special relationship arose because Plaintiff and the Class entrusted Defendant with their confidential PII and/or PHI, a necessary part of obtaining services from Defendant.

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

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

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

100. Defendant's own conduct created a foreseeable risk of harm to Plaintiff and the 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'sss misconduct also

included its decisions not to comply with industry standards for the safekeeping of the PII and PHI of Plaintiff and the Class, including basic encryption techniques freely available to Defendant.

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

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

103. Defendant had and continue to have a duty to adequately disclose that the PII and PHI of Plaintiff and the 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 Class to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their PII and/or PHI by third parties.

104. Defendant had a duty to employ proper procedures to prevent the unauthorized dissemination of the PII and/or PHI of Plaintiff and the Class.

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

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

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

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

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

110. Defendant breached its duty to exercise appropriate clearinghouse practices by failing to remove PII and/or PHI they were no longer required to retain pursuant to regulations.

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

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

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

114. As a direct and proximate result of Defendant's negligence, Plaintiff and the 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/or PHI is used; (iii) the compromise, publication, and/or theft of their PII and/or 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/or PHI; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the present and continuing 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/or 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/or PHI of Plaintiff and the Class; and (viii) present and continuing costs in terms of time, effort, and money that has been and will be expended to prevent, detect, contest, and repair the impact of the PII and/or PHI compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and the Class.

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

116. Additionally, as a direct and proximate result of Defendant's negligence, Plaintiff and the Class have suffered and will suffer the continued risks of exposure of their PII and/or 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/or PHI in its continued possession.

117. As a direct and proximate result of Defendant's negligence, Plaintiff and the Class

are entitled to recover actual, consequential, and nominal damages.

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

118. Plaintiff and the Class repeat and re-allege each and every allegation in the Complaint as if fully set forth herein.

119. Plaintiff and the Class entrusted their PII and/or PHI to Defendant. In so doing, Plaintiff and the Class entered into implied contracts with Defendant by which Defendant agreed to safeguard and protect such information, to keep such information secure and confidential, and to timely and accurately notify Plaintiff and the Class if their data had been breached and compromised or stolen.

120. In their Privacy Policy, Defendant represented that they had a legal duty to protect Plaintiff's and Class Member's PII and PHI.

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

122. Defendant breached the implied contracts it made with Plaintiff and the Class by failing to safeguard and protect their personal information, by failing to delete the information of Plaintiff and the Class once the relationship ended, and by failing to provide timely and accurate notice to them that personal information was compromised as a result of the Data Breach.

123. As a direct and proximate result of Defendant's above-described breach of implied contract, Plaintiff and the 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.

124. As a direct and proximate result of Defendant's above-described breach of implied contract, Plaintiff and the Class are entitled to recover actual, consequential, and nominal damages.

COUNT III
Breach of Fiduciary Duty
(On behalf of Plaintiff and the Nationwide Class)

125. Plaintiff fully incorporates by reference all of the above paragraphs, as though fully set forth herein.

126. In providing their PII and PHI to Defendant, Plaintiff and Class members justifiably placed a special confidence in Defendant to act in good faith and with due regard for the interests of Plaintiff and Class members to safeguard and keep confidential that PII and PHI.

127. Defendant accepted the special confidence Plaintiff and Class members placed in it, as evidenced by its acknowledgement that it had a legal duty to protect Plaintiff's and Class Members' PII and PHI.

128. In light of the special relationship between Defendant and Plaintiff and Class members, whereby Defendant became a guardian of Plaintiff and Class members' PII and PHI, Defendant became a fiduciary by its undertaking and guardianship of the PII and PHI, to act primarily for the benefit of its patients, including Plaintiff and Class members, for the safeguarding of Plaintiff and Class members' PII and PHI.

129. Defendant has a fiduciary duty to act for the benefit of Plaintiff and Class

members upon matters within the scope of its customer relationships, in particular, to keep secure the PII and PHI of its patients.

130. Defendant breached its fiduciary duties to Plaintiff and Class members by failing to protect the integrity of the systems containing Plaintiff and Class members' PII and PHI.

131. Defendant breached its fiduciary duties to Plaintiff and Class members by otherwise failing to safeguard Plaintiff and Class members' PII and PHI.

132. As a direct and proximate result of Defendant's breaches of its fiduciary duties, Plaintiff and Class members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the compromise, publication, and/or theft of their PII and PHI; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their PII and PHI; (iv) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (v) the continued risk to their PII and PHI, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII and PHI in its continued possession; (vi) future costs in terms of time, effort, and money that will be expended as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members; and (vii) the diminished value of the services they paid for and received.

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

COUNT IV

Unjust Enrichment
(On behalf of Plaintiff and the Nationwide Class)

134. Plaintiff and the Class repeat and re-allege each and every allegation in the Complaint as if fully set forth herein.

135. This cause of action is brought in the alternative to Plaintiff's breach of implied contract claim.

136. Plaintiff and Class members conferred a monetary benefit on Defendant, by providing Defendant with their valuable PII and PHI.

137. Defendant enriched itself by saving the costs they reasonably should have expended on data security measures to secure Plaintiff's and Class members' PII and PHI.

138. Instead of providing a reasonable level of security that would have prevented the Data Breach, Defendant instead calculated to avoid its data security obligations at the expense of Plaintiff and Class members by utilizing cheaper, ineffective security measures. Plaintiff and Class members, on the other hand, suffered as a direct and proximate result of Defendant's failure to provide the requisite security.

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

140. Defendant acquired the monetary benefit and PII and PHI through inequitable means in that it failed to disclose the inadequate security practices previously alleged.

141. If Plaintiff and Class members knew that Defendant had not secured their PII and PHI, they would not have agreed to provide their PII and PHI to Defendant.

142. Plaintiff and Class members have no adequate remedy at law.

143. As a direct and proximate result of Defendant's conduct, Plaintiff and Class members have suffered and will suffer injury, including but not limited to: (i) 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, 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 identity theft; (vi) 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 PII and PHI in their continued possession and (vii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII and PHI compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class members.

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

145. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and Class members, proceeds that they unjustly received from them.

VII. PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of herself and Class Members, request 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 each 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;

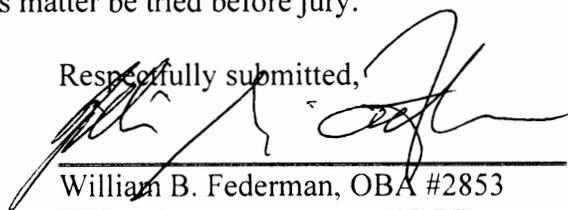
- xvi. requiring Defendant to implement logging and monitoring programs sufficient to track traffic to and from Defendant's servers; and for a period of 10 years, appointing a qualified and independent third party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendant's 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, but not limited to, actual, consequential, and nominal 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 jury.

Dated: June 16, 2022

Respectfully submitted,



William B. Federman, OBA #2853

FEDERMAN & SHERWOOD

10205 N. Pennsylvania Ave.

Oklahoma City, OK 73120

Phone: (405) 235-1560 | Fax: (405) 239-2112

wbf@federmanlaw.com

Counsel for Plaintiff and the Putative Class