MARTIN A. MUCKLEROY (martin@muckleroylunt.com)
MUCKLEROY LUNT, LLC
Nevada Bar No. 009634
6077 S. Fort Apache Road, Suite 140
Las Vegas, NV 89148
Tel: (702) 907-0097
Fax: (702) 938-4065

AMBER L. SCHUBERT (aschubert@sjk.law) (*pro hac vice* forthcoming)
SCHUBERT JONCKHEER & KOLBE LLP
2001 Union Street, Suite 200
San Francisco, CA 94123
Tel: (415) 788-4220
Fax: (415) 788-0161

Counsel for Plaintiff

UNITED STATES DISTRICT COURT

DISTRICT OF NEVADA

ANDREA KAY, on behalf of herself and all others similarly situated,

Plaintiff,

v.

PERRY JOHNSON & ASSOCIATES, INC. and BON SECOURS MERCY HEALTH, INC., d/b/a MERCY HEALTH,

Defendants.

No.

CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

Upon personal knowledge as to her own acts, and based upon her investigation, her counsel's investigation, and information and belief as to all other matters, Plaintiff Andrea Kay, on behalf of herself and all others similarly situated, alleges as follows:

INTRODUCTION

1. This action arises out of a targeted cyberattack and data breach caused by Defendants' failure to secure and safeguard Plaintiff's and other individuals' personally identifying information ("PII") and/or personal health information ("PHI"), including, at least, their names, dates of birth, addresses, medical record numbers, other health information, Social Security Numbers and medical testing results (the "Data Breach").

2. Between March 27, 2023 and May 2, 2023, a cyber intruder gained access to the network systems of Perry Johnson & Associates, Inc. ("PJA"), a third-party vendor of health information management technology to medical providers.

3. The unauthorized party obtained files from PJ&A containing the PII and PHI of approximately 9 million patients, including information provided to PJ&A by defendant Bon Secours Mercy Health, Inc., d/b/a Mercy Health ("Mercy Health"), a PJ&A client.

4. Plaintiff was a patient of Mercy Health. Plaintiff learned of the Data Breach when she received a notice from PJ&A dated November 8, 2023, almost 8 months after the Data Breach began, stating that Plaintiff's PII and/or PHI was exposed in the Data Breach.

5. The Data Breach was a direct result of the failure by Defendants to implement reasonable cyber-security procedures to protect the PII and PHI of Plaintiff and the Class and Subclass, as defined below.

6. Plaintiff, individually and on behalf of all others similarly situated, alleges claims under the Ohio Consumer Sales Practices Act, Ohio Rev. Code §§ 1345.01 *et seq*., the Ohio Deceptive Trade Practices Act, Ohio Rev. Code §§ 4165.01 *et seq*., and for negligence, negligent misrepresentation, unjust enrichment, and breach of implied contract.

7. Plaintiff, individually and on behalf of all others similarly situated, asks the Court to compel Defendants to adopt reasonable information security practices to secure the sensitive

PII and PHI that Defendants collect and store in their databases and to grant such other relief as the Court deems just and proper.

PARTIES

Plaintiff

8. Plaintiff Andrea Kay obtained medical services from medical facilities in the Cincinnati, OH area managed by Mercy Health. Plaintiff received a notice from PJ&A dated November 8, 2023 that her PII and/or PHI had been compromised. Plaintiff is a citizen of Kentucky.

Defendants

9. Defendant PJ&A is a Nevada corporation with its principal place of business at 1489 W. Warm Springs Road, Henderson, NV 89014. PJ&A provides transcription services to health care organizations and physicians for dictating and transcribing patient notes. PJ&A is a citizen of Nevada.

10. Defendant Mercy Health is an Ohio corporation with its principal place of business at 1701 Mercy Health Place, Cincinnati, OH 45237. Mercy Health operates hospitals and clinics throughout Ohio. Mercy Health is a citizen of Ohio.

JURISDICTION AND VENUE

11. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million, exclusive of interest and costs. The putative class contains millions of members, many of whom have citizenship diverse from Defendants.

12. This Court has jurisdiction over PJ&A because its principal place of business is in the District of Nevada, it operates in this District, and the computer systems implicated in the Data Breach are likely based in this District. Through its business operations in this District, PJ&A intentionally avails itself of the markets within this District such that the exercise of jurisdiction by this Court is just and proper.

13. This Court has jurisdiction over Defendant Mercy Health because it transacts business within this state and makes or performs contracts within this state.

14. Venue is proper under 28 U.S.C. § 1391(b)(1) because PJ&A resides in Nevada. Venue is also proper under 28 U.S.C. § 1391(b)(2) because a substantial part of the events or omissions giving rise to this action occurred in this District. PJ&A is based in this District, maintains customer PII and PHI in the District, and has caused harm to Plaintiff and the Class members residing in this District.

SUBSTANTIVE ALLEGATIONS

I. The Data Breach.

15. Plaintiff obtained medical services from medical facilities in the Cincinnati, OH area managed by Mercy Health.

16. In the regular course of its business, Mercy Health collects and maintains the PII and PHI of its current and former patients.

17. Mercy Health required Plaintiff and other Class members to provide their PII and PHI in connection with receiving healthcare services.

18. On information and belief, Mercy Health used PJ&A as a third-party vendor and provided, and continues to provide, patient data to PJ&A.

19. According to a notice issued to Plaintiff by PJ&A dated November 8, 2023, between March 27, 2023 and May 2, 2023, "[a]n unauthorized party gained access to the PJ&A network . . . and, during that time, acquired copies of certain files from PJ&A systems."

20. According to the notice received by Plaintiff, the PII and PHI exposed in the breach included names, dates of birth, addresses, medical record numbers, and other health information of affected patients.

21. Another disclosure concerning the Data Breach by PJ&A and posted on Mercy Health's website stated that for "some individuals, however, the impacted data may have also included Social Security numbers, insurance information and clinical information from medical

transcription files, such as laboratory and diagnostic testing results, medications, the name of the treatment facility, and the name of healthcare providers."

22. The scope of the Data Breach is massive. According to published reports, the Data Breach compromised the PII and PHI of nearly 9 million individuals.

II. Defendants Had a Duty to Secure Plaintiff's Information.

23. As a regular and necessary part of their businesses, Defendants collect highly sensitive PII and PHI of patients.

24. Defendants had duties to ensure that all information they collected and stored was secure, and that they maintained adequate and commercially reasonable data security practices to ensure the protection of Plaintiff's and the Class members' PII and PHI.

25. Defendants are covered under the Health Insurance Portability and Accountability Act ("HIPAA").

26. As covered entities under HIPAA, Defendants are required under federal and state law to maintain the strictest confidentiality of patients' PII and PHI that they acquire, receive, and collect, and Defendants are further required to maintain sufficient safeguards to protect that PII and PHI from being accessed by unauthorized third parties.

27. Defendants are subject to the rules and regulations for safeguarding electronic forms of medical information pursuant to the Health Information Technology Act ("HITECH"). *See* 42 U.S.C. §17921, 45 C.F.R. § 160.103. These rules establish national standards for the protection of patient information, including protected health information, defined as "individually identifiable health information" which either "identifies the individual" or where there is a "reasonable basis to believe the information can be used to identify the individual," that is held or transmitted by a healthcare provider. *See* 45 C.F.R. § 160.103.

28. HIPAA limits the permissible uses of "protected health information" and prohibits unauthorized disclosures of "protected health information."

29. HIPAA requires that Defendants implement appropriate safeguards for this information.

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

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

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

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

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

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

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

36. PJ&A's website states as follows: "PJ&A recognizes the importance of information security. Comprehensive policies and procedures are used to ensure that all access to patient data is restricted."

37. Mercy Health's Notice of Privacy Practices, posted on its website, states as follows: "Mercy Health is committed to protecting medical information about you. We create a record of the medical care and services you receive at Mercy Health sites for use in your care and treatment. We need this record to provide you with quality care and to comply with certain legal requirements."

38. Mercy Health's Notice of Privacy Practices continues: "This Notice applies to all the records of your care relating to services provided in the hospitals, outpatient and ambulatory care centers and other facilities that comprise Mercy Health, as well as the physicians and other health care professionals who provide services within those facilities, whether made by employees of Mercy Health or your personal doctor."

III. Defendants Failed to Comply with Reasonable Cybersecurity Standards.

39. Defendants knew or should have known the significance and necessity of safeguarding patients' PII and PHI and the foreseeable consequences of a data breach.

40. Defendants knew or should have known that because they collected and maintained the PII and PHI for a significant number of patients, a significant number of patients would be harmed by a breach of their systems.

41. Because PII and PHI is so sensitive and cyberattacks have become a rising threat, the Federal Trade Commission ("FTC") has issued numerous guides for businesses holding sensitive information and emphasized the importance of adequate data security practices.

42. The FTC also stresses that appropriately safeguarding information held by businesses should be factored into all business-related decision making.

43. The FTC has also issued guidance for addressing the devastating results of data breaches and their harmful effects, warning: "Once identity thieves have your personal information, they can drain your bank account, run up charges on your credit cards, open new utility accounts, or get medical treatment on your health insurance."

44. An FTC Publication titled "Protecting Personal Information: A Guide for Business" lays out fundamental data security principles and standard practices that businesses should implement.[1] The guidelines highlight that businesses should (a) protect the personal customer information they collect and store; (b) properly dispose of personal information that is no longer needed; (c) encrypt information stored on their computer networks; (d) understand their network's vulnerabilities; and (e) implement policies to correct security problems.

45. The FTC also recommends that businesses use an intrusion detection system, monitor all incoming traffic to the networks for unusual activity, monitor for large amounts of data being transmitted from their systems, and have a response plan prepared in the event of a breach.

46. The FTC also recommends that businesses limit access to sensitive information, require complex passwords to be used on the 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—a step that would have been particularly prudent in light of the methods used by the perpetrators in this case.

47. Businesses that do not comply with the basic protection of sensitive information are facing enforcement actions brought by the FTC.

[1] https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business.

48. Failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data is an unfair act or practice prohibited pursuant to Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45.

49. Many states' unfair and deceptive trade practices statutes are similar to the FTC Act, and many states adopt the FTC's interpretations of what constitutes an unfair or deceptive trade practice.

50. Defendants knew or should have known of their obligation to implement appropriate measures to protect patients' PII and PHI but failed to comply with the FTC's basic guidelines and other industry best practices, including the minimum standards set by the National Institute of Standards and Technology Cybersecurity Framework Version 1.1.[2]

51. Defendants' failures to employ reasonable measures to adequately safeguard against unauthorized access to PII and PHI constitute an unfair act or practice as prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45, as well as by state statutory analogs.

52. Defendants failed to use reasonable care in maintaining the privacy and security of Plaintiff's and the Class members' PII and PHI. If Defendants had implemented adequate security measures, cybercriminals could never have accessed the PII and PHI of Plaintiff and the Class members, and the Data Breach would have either been prevented or much smaller in scope.

53. Due to the sensitive nature of the PII and PHI accessed in the Data Breach, cybercriminals can commit identity theft, financial fraud, and other identity-related fraud against Plaintiff and the Class members now and indefinitely in the future. As a result, Plaintiff and the Class members have suffered injury and face an imminent and substantial risk of further injury including identity theft and related cybercrimes due to the Data Breach.

54. The Data Breach exposed PII and PHI that is both valuable and highly coveted on underground markets because it can be used to commit identity theft and financial fraud.

55. Identity thieves use such information to, among other things, gain access to bank accounts, social media accounts, and credit cards. Identity thieves can also use it to open new

[2] https://nvlpubs.nist.gov/nistpubs/cswp/nist.cswp.04162018.pdf.

financial accounts, open new utility accounts, obtain medical treatment using victims' health insurance, file fraudulent tax returns, obtain government benefits, obtain government identification cards, or create "synthetic identities." Additionally, identity thieves often wait significant amounts of time—months or even years—to use the information obtained in data breaches because victims often become less vigilant in monitoring their accounts as time passes, therefore making the stolen information easier to use without detection. These identity thieves will also re-use stolen data, resulting in victims of one data breach suffering the effects of several cybercrimes from one instance of unauthorized access to their PII or PHI.

56. Victims of data breaches are much more likely to become victims of identity fraud than those who have not. Data Breach victims who do experience identity theft often spend hundreds of hours fixing the damage caused by identity thieves.[3]

57. Additionally, the U.S. Department of Justice Bureau of Justice Statistics has reported that, even if data thieves have not caused financial harm, data breach victims "reported spending an average of about 7 hours clearing up the issues."[4]

58. Social Security numbers 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 to change. The Social Security Administration stresses that the loss of an individual's Social Security number can lead to identity theft and extensive financial fraud:

> Identity theft is one of the fastest growing crimes in America. 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, when 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.[5]

[3] https://www.marylandattorneygeneral.gov/ID%20Theft%20Documents/Identitytheft.pdf.
[4] https://bjs.ojp.gov/content/pub/pdf/vit14.pdf.
[5] https://www.ssa.gov/pubs/EN-05-10064.pdf.

59. The information compromised in the Data Breach—including Social Security numbers—is much more valuable than the loss of credit card information in a retailer data breach. There, victims can simply close their credit and debit card accounts and potentially even rely on automatic fraud protection offered by their banks. Here, however, the information compromised is much more difficult, if not impossible, for consumers to re-secure after being stolen.

IV. Defendants Failed to Provide Proper Notice.

60. The HIPAA Breach Notification Rule, 45 C.F.R. §§ 164.400-414, also requires HIPAA covered entities and their business associates, like Defendants, to provide notification following a breach of unsecured protected health information, which includes protected health information that is not rendered unusable, unreadable, or indecipherable to unauthorized persons— i.e. non-encrypted data—to each affected individual "without unreasonable delay and ***in no case later than 60 days following discovery of the breach***." (emphasis added)

61. Should a health care provider experience an unauthorized disclosure, it is required to conduct a risk assessment under HIPAA, as follows: "A covered entity or business associate must now undertake a four-factor risk assessment to determine whether or not PHI has been compromised and overcome the presumption that the breach must be reported." The four-factor risk assessment focuses on: (1) the nature and extent of the PHI involved in the incident (e.g., whether the incident involved sensitive information like social security numbers or infectious disease test results); (2) the recipient of the PHI; (3) whether the PHI was actually acquired or viewed; and, (4) the extent to which the risk that the PHI was compromised has been mitigated following unauthorized disclosure (e.g., whether it was immediately sequestered and destroyed).

62. Although the breach reportedly began as early as March 27, 2023, and was reportedly discovered by PJ&A on or about July 21, 2023, Plaintiff did not receive notice of the breach until on or about November 8, 2023.

V. Plaintiff's Experiences.

63. In the course of her treatment at one or more Mercy Health facilities, Plaintiff provided her sensitive PII and PHI to Mercy Health.

64. Plaintiff took reasonable steps to maintain the confidentiality of her PII and PHI. Plaintiff relied on Mercy Health's representations, experience, and sophistication to keep her information secure and confidential.

65. As a result of the Data Breach, Plaintiff was forced to take measures to mitigate the harm, including spending time monitoring her credit and financial accounts, researching the Data Breach, and researching and taking steps to prevent and mitigate the likelihood of identity theft, among other harms.

66. As a result of the Data Breach, Plaintiff and the Class members have suffered actual injuries including: (a) paying money to Defendants, which they would not have done had Defendants disclosed that they lacked data security practices adequate to safeguard information; (b) damages to and diminution in the value of Plaintiff's PII and PHI—property that Plaintiff entrusted to Defendants in receiving services; (c) loss and invasion of Plaintiff's privacy; and (d) injuries arising from the increased risk of fraud and identity theft, including the cost of taking reasonable identity theft protection measures, which will continue for years.

VI. Plaintiff and the Class Face Substantial Harms Caused by the Data Breach.

67. Plaintiff and the Class members face a lifetime of constant surveillance of their financial, personal, and health records; monitoring; loss of reputation; and loss of rights. Plaintiff and the Class are incurring and will continue to incur such damage in addition to any fraudulent use of their PII/PHI.

68. PII/PHI is very valuable to criminals, as evidenced by the prices they will pay for it on the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information is sold at prices ranging from $40 to $200, and bank details have a price range of $50 to $200.[6]

69. Consumers place a high value on the privacy of that data, as they should. Researchers shed light on how much consumers value their data privacy—and the amount is

[6] *Your Personal Data Is for Sale on the Dark Web. Here's How Much It Costs,* DIGITAL TRENDS (Oct. 16, 2019), https://www.digitaltrends.com/computing/personal-data-sold-on- the-dark-web-how-much-it-costs.

considerable. Indeed, studies confirm that "when privacy information is made more salient and accessible, some consumers are willing to pay a premium to purchase from privacy protective websites."[7]

70. The information compromised in the Data Breach is significantly more valuable than the loss of, for example, payment card information in a retailer data breach because, in that situation, victims can cancel or close payment card accounts. The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change—name, birthdate, health insurance information, and health records.

71. Cyber criminals sell health information at a far higher premium than stand-alone PII. This is because health information enables thieves to go beyond traditional identity theft and obtain medical treatments, purchase prescription drugs, submit false bills to insurance companies, or even undergo surgery under a false identity.[8] The shelf life for this information is also much longer—while individuals can update their credit card numbers, they are less likely to change their Medicare numbers or health insurance information.

72. All-inclusive health insurance dossiers containing sensitive health insurance information, names, addresses, telephone numbers, email addresses, Social Security numbers, and bank account information, complete with account and routing numbers, can fetch up to $1,200 to $1,300 each on the black market.[9] According to a report released by the Federal Bureau of Investigation's ("FBI") Cyber Division, criminals can sell healthcare records for 50 times the price of a stolen Social Security or credit card number.[10]

---

[7] Janice Y. Tsai et al., *The Effect of Online Privacy Information on Purchasing Behavior, An Experimental Study*, 22(2) INFO. SYS. RSCH. 254 (June 2011) https://www.jstor.org/stable/23015560?seq=1.

[8] *Medical Identity Theft: FAQs for Health Care Providers and Health Plans*, FTC, https://www.ftc.gov/system/files/documents/plain-language/bus75-medical-identity-theft-faq-health-care-health-plan.pdf (last visited Aug. 22, 2023).

[9] *See* SC Staff, *Health Insurance Credentials Fetch High Prices in the Online Black Market*, SC MAG (July 16, 2013), https://www.scmagazine.com/news/breach/health-insurance-credentialsfetch- high-prices-in-the-online-black-market.

[10] *See* Federal Bureau of Investigation, *Health Care Systems and Medical Devices at Risk for Increased Cyber Intrusions for Financial Gain* (Apr. 8, 2014),

73. Identity thieves may use stolen data to commit health care fraud, prescription drug fraud, bank fraud, credit card fraud, employer or tax-related fraud, government documents or benefits fraud, loan or lease fraud, phone or utilities fraud, among other forms of fraud.[11]

74. Criminals can use stolen PII/PHI to extort a financial payment by "leveraging details specific to a disease or terminal illness."[12] Quoting Carbon Black's Chief Cybersecurity Officer, one recent article explained: "Traditional criminals understand the power of coercion and extortion. … By having healthcare information—specifically, regarding a sexually transmitted disease or terminal illness—that information can be used to extort or coerce someone to do what you want them to do."[13]

75. Cybercriminals can take the PII/PHI of Plaintiff and the Class members to engage in identity theft, healthcare fraud, and/or to sell it to other criminals who will purchase the PII/PHI for that purpose. The fraudulent activities resulting from the Data Breach may not come to light for years.

76. Theft of PII/PHI is serious. The FTC warns consumers that identity thieves use PII/PHI to exhaust financial accounts, receive medical treatment, start new utility accounts, and incur charges and credit in a person's name.[14]

77. While some identity theft victims can resolve their problems quickly, others spend hundreds of dollars and many days repairing damage to their good name and credit record. Some consumers victimized by identity theft may lose job opportunities or be denied loans for

---

https://www.illuminweb.com/wp-content/uploads/ill-mo-uploads/103/2418/health-systemscyber- intrusions.pdf.

[11] FTC Consumer Sentinel Network, Compare Identity Theft Report Types, https://public.tableau.com/app/profile/federal.trade.commission/viz/IdentityTheftReports/TheftTypesOverTime, (Last visited July 9, 2023).

[12] *See* Andrew Steager, *What Happens to Stolen Healthcare Data*, HEALTHTECH MAGAZINE (Oct. 20, 2019), https://healthtechmagazine.net/article/2019/10/what-happens-stolen-healthcaredata- perfcon ("What Happens to Stolen Healthcare Data") (quoting Tom Kellermann, Chief Cybersecurity Officer, Carbon Black, stating "Health information is a treasure trove for criminals.").

[13] *Id.*

[14] *See* Federal Trade Commission, *What to Know About Identity Theft*, FED. TRADE COMM'N CONSUMER INFO.

education, housing, or cars because of negative information on their credit reports. In rare cases, they may even be arrested for crimes they did not commit.

78. Identity theft, which costs Americans billions of dollars annually, occurs when an individual's PII is used without consent to commit fraud or other crimes. Victims of identity theft typically lose hundreds of hours dealing with the crime and hundreds, if not thousands, of dollars.

79. According to Javelin Strategy & Research, in 2018 alone, identity theft affected over 16.7 million individuals, causing a loss of over $16.8 billion.

80. Recent FTC data reveals that identify theft remains the top category of fraud reports received by the agency.[15] The FTC received over 1,100,000 reports of identity theft in 2022, and over 280,000 for the first quarter of 2023 alone.[16]

81. Identity thieves use personal information for various crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.[17] According to Experian, one of the largest credit reporting companies in the world, "[t]he research shows that personal information is valuable to identity thieves, and if they can get access to it, they will use it" to, among other things: open a new credit card or loan; change a billing address so the victim no longer receives bills; open new utilities; obtain a mobile phone; open a bank account and write bad checks; use a debit card number to withdraw funds; obtain a new driver's license or ID; or use the victim's information in the event of arrest or court action.[18]

---

[15] FTC Consumer Sentinel Network, Federal Trade Commission, https://public.tableau.com/app/profile/federal.trade.commission/viz/FraudandIDTheftMaps/AllReportsbyState, (Last visited July 9, 2023).

[16] *Id*.

[17] The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 12 C.F.R. § 1022.3(h). 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." 12 C.F.R. § 1022.3(g).

[18] *See* Susan Henson, *What Can Identity Thieves Do with Your Personal Information and How Can You Protect Yourself*, EXPERIAN, https://www.experian.com/blogs/ask-experian/what-canidentity- thieves-do-with-your-personal-information-and-how-can-you-protect-yourself/ (last accessed Mar. 21, 2022).

82. With access to an individual's PII, criminals can do more than just empty a victim's bank account. They can also commit all manner of fraud, including (i) obtaining a driver's license or official identification card in the victim's name but with the thief's picture; (ii) using the victim's name and SSN to obtain government benefits; or (iii) filing a fraudulent tax return using the victim's information. In addition, identity thieves may even give the victim's personal information to police during an arrest.[19]

83. Consumers place a high value not only on their personal information but also on the privacy of that data. They do so because identity theft causes "significant negative financial impact on victims" in addition to severe distress and other strong emotional and physical reactions.

84. The United States Government Accountability Office ("GAO") explains that "[t]he term 'identity theft' is broad and encompasses many types of criminal activities, including fraud on existing accounts—such as unauthorized use of a stolen credit card number—or fraudulent creation of new accounts—such as using stolen data to open a credit card account in someone else's name."[20] The GAO Report notes that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[21]

85. Further, as noted, there is the likelihood of a lapse in time between when the harm occurs to a victim of identity theft and when that harm is discovered, as well as a lapse between when the PII/PHI is stolen and when it is actually used. According to the GAO, which conducted a study regarding the growing number of data breaches:

> Further, as noted, there is the likelihood of a lapse in time between when the harm occurs to a victim of identity theft and when that harm is discovered, as

[19] *See* Federal Trade Commission, *Warning Signs of Identity Theft*, IDENTITYTHEFT.GOV https://www.identitytheft.gov/Warning-Signs-of-Identity-Theft (last accessed Mar. 21, 2023); *See* Identity Theft Resource Center, *2021 Consumer Aftermath Report*, IDENTITY THEFT RES.

[20] *See* Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown, U.S. Government Accountability Office Report to Congressional Requesters ("GAO Report") at 2 (June 2007), https://www.gao.gov/new.items/d07737.pdf, (Last visited July 10, 2023).

[21] *Id.*

> well as a lapse between when the PII/PHI is stolen and when it is actually used. According to the GAO, which conducted a study regarding the growing number of data breaches:

86. According to the FBI's Internet Crime Complaint Center (IC3) 2019 Internet Crime Report, Internet-enabled crimes reached their highest number of complaints and dollar losses in 2019, resulting in more than $3.5 billion in losses to individuals and business victims.[22]

87. Further, according to the same report, "rapid reporting can help law enforcement stop fraudulent transactions before a victim loses the money for good."[23] Defendants did not rapidly or timely report to Plaintiff and the Class members that their PII/PHI had been stolen.

88. As a result of the Data Breach, Plaintiff and the Class members' PII/PHI has been exposed to criminals for misuse. The injuries suffered by Plaintiff and the Class members, or likely to be suffered thereby as a direct result of the Data Breach, include:

a. unauthorized use of their PII/PHI;
b. theft of their personal, financial, and health information;
c. costs associated with the detection and prevention of identity theft and unauthorized use of their financial and healthcare accounts;
d. damages arising from the inability to use their PII/PHI;
e. improper disclosure of their PII/PHI;
f. loss of privacy and embarrassment;
g. loss of reputation;
h. trespass and damage their personal property, including PII/PHI;
i. the imminent and certainly impending risk of having their confidential medical information used against them by spam callers and/or hackers targeting them with phishing schemes to defraud them;

[22] *2019 Internet Crime Report Released*, FBI, https://www.fbi.gov/news/stories/2019-internet-crime-report-released-021120#:~:text=IC3%20received%20467%2C361%20complaints%20in,%2Ddelivery%20scams%2C%20and%20extortion. (Last visited September 11, 2023).

[23] *Id*.

j. costs associated with time spent and the loss of productivity or the enjoyment of one's life from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Data Breach, including finding fraudulent charges, purchasing credit monitoring and identity theft protection services, and the stress, nuisance, and annoyance of dealing with all issues resulting from the Data Breach;

k. the imminent and certainly impending injury flowing from potential fraud and identify theft posed by their PII/PHI being placed in the hands of criminals and already misused via the sale of Plaintiff and the Class members' information on the Internet black market; and

l. damages to and diminution in value of their PII/PHI entrusted to Defendants.

89. In addition to a remedy for economic harm, Plaintiff and the Class members maintain an interest in ensuring that their PII/PHI is secure, remains secure, and is not subject to further misappropriation and theft.

90. Defendants disregarded the rights of Plaintiff and the Class members by (i) intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure that their network servers were protected against unauthorized intrusions; (ii) failing to disclose that Defendants did not have adequately robust security protocols and training practices in place to adequately safeguard Plaintiff and the Class members' PII/PHI; (iii) failing to take standard and reasonably available steps to prevent the Data Breach; and (iv) failing to provide Plaintiff and the Class members prompt notice of the Data Breach.

91. The actual and adverse effects to Plaintiff and the Class members, including the imminent, immediate and continuing increased risk of harm for identity theft, identity fraud, and medical fraud directly or proximately caused by Defendants' wrongful actions or inaction and the resulting Data Breach require Plaintiff and the Class members to take affirmative acts to recover their peace of mind and personal security including, without limitation, purchasing credit reporting services, purchasing credit monitoring and/or internet monitoring services, frequently

obtaining, purchasing and reviewing credit reports, bank statements, and other similar information, instituting and/or removing credit freezes, and closing or modifying financial accounts, for which there is a financial and temporal cost. Plaintiff and other Class members have suffered, and will continue to suffer, such damages for the foreseeable future.

CLASS ACTION ALLEGATIONS

92. Plaintiff brings this action as a class action pursuant to Rules 23(a) and 23(b)(1)-(3) of the Federal Rules of Civil Procedure, on behalf of herself and a Nationwide Class, defined as follows:

> All persons in the United States whose PII and PHI was compromised in the Data Breach announced by PJ&A in November 2023, including all who were sent a notice of the Data Breach.

93. Plaintiff seeks certification of an Ohio Subclass, defined as follows:

> All persons in Ohio whose PII and PHI was compromised in the Data Breach announced by PJ&A in November 2023, including all who were sent a notice of the Data Breach.

94. Excluded from the Nationwide Class and the Subclass are governmental entities, Defendants, any entity in which Defendants have a controlling interest, and Defendants' officers, directors, affiliates, legal representatives, employees, coconspirators, successors, subsidiaries, and assigns. Also excluded are any judges, justices, or judicial officers presiding over this matter and the members of their immediate families and judicial staff.

95. This action is brought and may be properly maintained as a class action pursuant to Rule 23. This action satisfies the requirements of Rule 23, including numerosity, commonality, typicality, adequacy, predominance, and superiority.

96. **Numerosity.** The Nationwide Class and Subclass are so numerous that the individual joinder of all members is impracticable. While the Nationwide Class and Subclass members' exact number are currently unknown and can only be ascertained through appropriate discovery, on November 3, 2023, PJ&A notified the U.S Department of Health and Human Services that the Breach affected 8,952,212 individuals.

97. **Commonality.** Common legal and factual questions exist that predominate over any questions affecting only individual Nationwide Class or Subclass members. These common questions, which do not vary among Nationwide Class or Subclass members and which may be determined without reference to any Nationwide Class or Subclass member's individual circumstances, include, but are not limited to:

a. Whether Defendants knew or should have known that their systems were vulnerable to unauthorized access;

b. Whether Defendants failed to take adequate and reasonable measures to ensure their data systems were protected;

c. Whether Defendants failed to take available steps to prevent and stop the breach from happening;

d. Whether Defendants owed a legal duty to Plaintiff and Class and Subclass members to protect their PII and PHI;

e. Whether Defendants breached any duty to protect the personal information of Plaintiff and Class and Subclass members by failing to exercise due care in protecting their PII and PHI;

f. Whether Plaintiff and Class and Subclass members are entitled to actual, statutory, or other forms of damages and other monetary relief; and,

g. Whether Plaintiff and Class and Subclass members are entitled to equitable relief, including injunctive relief or restitution.

98. **Typicality.** Plaintiff's claims are typical of other Class members' claims because Plaintiff and the Class members were subjected to the same allegedly unlawful conduct and damaged in the same way.

99. **Adequacy of Representation.** Plaintiff is an adequate Nationwide Class and Subclass representative because she is a Nationwide Class and Subclass member, and her interests do not conflict with the Nationwide Class or Subclass' interests. Plaintiff retained counsel who are competent and experienced in class action and data breach litigation. Plaintiff and her counsel

intend to prosecute this action vigorously for the Nationwide Class and Subclass' benefit and will fairly and adequately protect their interests.

100. **Predominance and Superiority.** The Nationwide Class and Subclass can be properly maintained because the above common questions of law and fact predominate over any questions affecting individual Nationwide Class or Subclass members.

101. A class action is also superior to other available methods for the fair and efficient adjudication of this litigation because individual litigation of each Nationwide Class and Subclass member's claim is impracticable. Even if each Nationwide Class or Subclass member could afford individual litigation, the court system could not. It would be unduly burdensome if thousands of individual cases proceed. Individual litigation also presents the potential for inconsistent or contradictory judgments, the prospect of a race to the courthouse, and the risk of an inequitable allocation of recovery among those with equally meritorious claims. Individual litigation would increase the expense and delay to all parties and the courts because it requires individual resolution of common legal and factual questions. By contrast, the class-action device presents far fewer management difficulties and provides the benefit of a single adjudication, economies of scale, and comprehensive supervision by a single court.

102. **Declaratory and Injunctive Relief.** The prosecution of separate actions by individual Class and Subclass members would create a risk of inconsistent or varying adjudications with respect to individual Class and Subclass members that would establish incompatible standards of conduct for Defendant. Such individual actions would create a risk of adjudications that would be dispositive of the interests of other Class or Subclass members and impair their interests. Defendants have acted and/or refused to act on grounds generally applicable to the Class, making final injunctive relief or corresponding declaratory relief appropriate.

CLAIMS FOR RELIEF

Count 1
Violation of the Ohio Consumer Sales Practices Act
On behalf of Plaintiff and the Ohio Subclass Against All Defendants

103. Plaintiff incorporates by reference and realleges each and every allegation above as though fully set forth herein.

104. Plaintiff brings this claim on behalf of herself and the Ohio Subclass.

105. Plaintiff is a "person," as defined by Ohio Rev. Code § 1345.01(B).

106. Defendants were "suppliers" engaged in "consumer transactions," as defined by Ohio Rev. Code §§ 1345.01(A) & (C).

107. Defendants advertised, offered, or sold goods or services in Ohio and engaged in trade or commerce directly or indirectly affecting the people of Ohio.

108. Defendants engaged in unfair and deceptive acts and practices in connection with a consumer transaction, in violation of Ohio Rev. Code § 1345.02, including: (a) representing that the subject of a transaction had approval, performance characteristics, uses, and benefits that it did not have, and (b) representing that the subject of a transaction was of a particular standard or quality when they were not.

109. Defendants engaged in unconscionable acts and practices in connection with a consumer transaction, in violation of Ohio Rev. Code § 1345.03, including: (a) knowingly taking advantage of the inability of Plaintiff to reasonably protect her interest because of their ignorance of the issues discussed herein; (b) knowing at the time the consumer transaction was entered into of the inability of the consumer to receive a substantial benefit from the subject of the consumer transaction; (c) requiring the consumer to enter into a consumer transaction on terms the supplier knew were substantially one-sided in favor of the supplier; and (d) knowingly making a misleading statement of opinion on which the consumer was likely to rely to the consumer's detriment.

110. Defendants' unfair, deceptive, and unconscionable acts and practices include: (a) failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's information, which was a direct and proximate cause of the Data Breach; (b) failing to identify and remediate foreseeable security and privacy risks and sufficiently improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate

cause of the Data Breach; (c) failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's PII and PHI, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach; (d) misrepresenting that it would protect the privacy and confidentiality of Plaintiff's PII and PHI, including by implementing and maintaining reasonable security measures; (e) misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's PII and PHI, including duties imposed by the FTC Act, 15 U.S.C. § 45; (f) omitting, suppressing, and concealing the material fact that it did not properly secure Plaintiff's PII and PHI; and (g) omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's PII and PHI, including duties imposed by the FTC Act, 15 U.S.C. § 45.

111. Defendants' representations and omissions were material because they deceived Plaintiff, and were likely to deceive other reasonable consumers, about the adequacy of Defendants' data security and ability to protect the confidentiality of consumers' PII and PHI.

112. Defendants intended to mislead Plaintiff and induce her to rely on their misrepresentations and omissions.

113. Defendants acted intentionally, knowingly, and maliciously to violate Ohio's Consumer Sales Practices Act, and recklessly disregarded Plaintiff's rights.

114. Defendants' unfair, deceptive, and unconscionable acts and practices complained of herein affected the public interest, including the many Ohioans affected by the Data Breach.

115. As a direct and proximate result of Defendants' unfair, deceptive, and unconscionable acts and practices, Plaintiff has suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, as alleged herein, including but not limited to fraud and identity theft; time and expenses related to monitoring her financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of her PII and PHI; overpayment for Defendants' services; loss of the

value of access to her PII and PHI, and the value of identity protection services made necessary by the Data Breach.

116. Pursuant to Ohio Rev. Code § 1345.09(A), Plaintiff, individually, seeks actual economic damages and non-economic damages of up to five thousand dollars.

117. Pursuant to Ohio Rev. Code § 1345.09(D), Plaintiff seeks declaratory and injunctive relief.

118. Pursuant to Ohio Rev. Code § 1345.09(F), Plaintiff seeks an award of reasonable attorneys' fees.

Count 2
Violation of the Ohio Deceptive Trade Practices Act
On behalf of Plaintiff and the Ohio Subclass Against All Defendants

119. Plaintiff incorporates by reference and realleges each and every allegation above as though fully set forth herein.

120. Plaintiff brings this claim on behalf of herself and the Ohio Subclass.

121. Plaintiff, Defendants and Ohio Subclass members are "persons" as defined by Ohio Rev. Code § 4165.01(D).

122. Defendants advertised, offered, or sold goods or services in Ohio and engaged in trade or commerce directly or indirectly affecting the people of Ohio.

123. Defendants engaged in deceptive trade practices in the course of their businesses and vocations, in violation of Ohio Rev. Code § 4165.02, including: (a) representing that their goods and services have approval, characteristics, uses, or benefits that they do not have; (b) representing that their goods and services are of a particular standard or quality when they are of another; and (c) advertising their goods and services with intent not to sell them as advertised.

124. Defendants' deceptive trade practices include: (a) failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's and the Ohio Subclass members' PII and PHI, which was a direct and proximate cause of the Data Breach; (b) failing to identify and remediate foreseeable security and privacy risks and sufficiently improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and

proximate cause of the Data Breach; (c) failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and the Ohio Subclass members' PII and PHI, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach; (d) misrepresenting that they would protect the privacy and confidentiality of Plaintiff's and the Ohio Subclass members' PII and PHI, including by implementing and maintaining reasonable security measures; (e) misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and the Ohio Subclass members' PII and PHI, including duties imposed by the FTC Act, 15 U.S.C. § 45; (f) omitting, suppressing, and concealing the material fact that they did not properly secure Plaintiff's and the Ohio Subclass members' PII and PHI; and (g) omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and the Ohio Subclass members' PII and PHI, including duties imposed by the FTC Act, 15 U.S.C. § 45.

125. Defendants' representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendants' data security and ability to protect the confidentiality of consumers' PII and PHI.

126. Defendants intended to mislead Plaintiff and the Ohio Subclass members and induce them to rely on their misrepresentations and omissions.

127. Defendants acted intentionally, knowingly, and maliciously to violate Ohio's Deceptive Trade Practices Act, and recklessly disregarded Plaintiff's and the Ohio Subclass members' rights.

128. As a direct and proximate result of Defendants' deceptive trade practices, Plaintiff and the Ohio Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, as alleged herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their PII and PHI; overpayment for Defendants' services; loss of the value of

access to their PII and PHI; and the value of identity protection services made necessary by the Data Breach.

129. Plaintiff and the Ohio Subclass members seek all monetary and non-monetary relief allowed by law, including injunctive relief, actual damages, attorneys' fees, and any other relief that is just and proper.

Count 3
Negligence
On behalf of Plaintiff and the Nationwide Class Against All Defendants

130. Plaintiff incorporates by reference and realleges each and every allegation above as though fully set forth herein.

131. Plaintiff and the Class members were required to provide their PII and PHI, including their names, dates of birth, addresses, telephone numbers, email addresses, and Social Security numbers, to Defendants as a condition of obtaining treatment.

132. Plaintiff and the Class members entrusted their PII and PHI to Defendants with the understanding that Defendants would safeguard their PII.

133. In their written privacy policies, Defendants expressly promised Plaintiff and the Class members that they would only disclose PII and PHI under certain circumstances, none of which relate to the Defendants Data Breach.

134. In addition, Defendants promised to maintain reasonable and appropriate safeguards to protect Plaintiff's and the Class members' PII and PHI.

135. Defendants had full knowledge of the sensitivity of the PII and PHI that they stored and the types of harm that Plaintiff and the Class members could and would suffer if that PII and PHI were wrongfully disclosed.

136. Defendants violated their duty to implement and maintain reasonable security procedures and practices.

137. That duty included, among other things, designing, maintaining, and testing Defendants' information security controls to ensure that PII and PHI in their possession was adequately secured by, for example, encrypting sensitive personal information, installing

intrusion detection systems and monitoring mechanisms, and using access controls to limit access to sensitive data.

138. Defendants' duty of care arose from, among other things,

a. Defendants' exclusive ability (and the Class members' inability) to ensure that their systems were sufficient to protect against the foreseeable risk that a data breach could occur;

b. Section 5 of the FTC Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, failing to adopt reasonable data security measures;

c. Defendants' common law duties to adopt reasonable data security measures to protect PII and PHI and to act as a reasonable and prudent person under the same or similar circumstances would act; and

d. State statutes requiring reasonable data security measures, including Nev. Rev. Stat. § 603A.210, which states that businesses possessing personal information of Nevada residents "shall implement and maintain reasonable security measures to protect those records from unauthorized access."

139. Defendants' violations of the FTC Act and state data security statutes constitute negligence per se for purposes of establishing the duty and breach elements of Plaintiff's negligence claim. Those statutes were designed to protect a group to which Plaintiff belongs and to prevent the types of harm that resulted from the Data Breach.

140. Defendants are companies that had the financial and personnel resources necessary to prevent the Data Breach. Defendants nevertheless failed to adopt reasonable data security measures, in breach of the duties it owed to Plaintiff and the Class members.

141. Plaintiff and the Class members were the foreseeable victims of Defendants' inadequate data security.

142. Defendants knew that a breach of its systems could and would cause harm to Plaintiff and the Class members.

143. Defendants' conduct created a foreseeable risk of harm to Plaintiff and the Class members. Defendants' conduct included their failure to adequately restrict access to their patient records' database, which held patients' PII and PHI.

144. Defendants knew or should have known of the inherent risks in collecting and storing massive amounts of PII and PHI, the importance of providing adequate data security over that PII, and the frequent cyberattacks within the healthcare industry.

145. Plaintiff and the Class members had no ability to protect their PII and PHI once it was in Defendants' possession and control. Defendants were in an exclusive position to protect against the harm suffered by Plaintiff and the Class members as a result of the Data Breach.

146. Defendants, through their actions and inactions, breached their duty owed to Plaintiff and the Class members by failing to exercise reasonable care in safeguarding their PII and PHI while it was in Defendants' possession and control.

147. Defendants breached their duty by, among other things, their failure to adopt reasonable data security practices and failure to adequately encrypt the PII and PHI in its systems.

148. Defendants inadequately safeguarded patients' PII and PHI in deviation of standard industry rules, regulations, and best practices at the time of the Data Breach. But for Defendants' breaches of their duty to adequately protect Plaintiff's and the Class members' PII and PHI, the information would not have been stolen.

149. There is a temporal and close causal connection between Defendants' failure to implement adequate data security measures, the Data Breach, and the harms suffered by Plaintiff and the Class members. As a result of Defendants' negligence, Plaintiff and the Class members suffered and will continue to suffer the various types of damages alleged herein.

150. Plaintiff and the Class members are entitled to all forms of monetary compensation set forth herein, including monetary payments to provide adequate identity protection services. Plaintiff and the Class members are also entitled to the injunctive relief sought herein.

Count 4
Negligent Misrepresentation
On behalf of Plaintiff and the Nationwide Class Against All Defendants

151. Plaintiff incorporates by reference and realleges each and every allegation above as though fully set forth herein.

152. Nevada has adopted the Restatement (Second) of Torts § 551 (1977), which imposes liability for negligent misrepresentations based on omissions. Section 551, titled "Liability for Nondisclosure," states:

> One who fails to disclose to another a fact that he knows may justifiably induce the other to act or refrain from acting in a business transaction is subject to the same liability to the other as though he had represented the nonexistence of the matter that he has failed to disclose, if […] he is under a duty to the other to exercise reasonable care to disclose the matter in question.

153. Defendants failed to disclose to Plaintiff and the Class members that they did not employ reasonable measures to protect patients' PII and PHI.

154. Defendants knew or should have known that their data security practices were deficient. This is true because, among other things, Defendants were aware that the healthcare industry is a frequent target of sophisticated cyberattacks.

155. Defendants' omissions were material given the sensitivity of the PII and PHI maintained by Defendants and the gravity of the harm that could result from the theft thereof.

156. Because of the relationship between the parties, patients would reasonably expect a disclosure of Defendants' inadequate data security.

157. Had Defendants disclosed their inadequate data security to Plaintiff and the Class members, they would not have entrusted their PII and PHI to Defendants.

158. Defendants should have made a proper disclosure to patients as part of the purchase of goods or services, or by any other means reasonably calculated to inform consumers of their inadequate data security.

159. In addition to their omissions, Defendants are also liable for their implied misrepresentations.

160. Defendants required consumers to provide their PII and PHI during treatment. In doing so, Defendants made implied or implicit representations that they employed reasonable data security practices to protect consumers' PII and PHI.

161. By virtue of accepting Plaintiff's and the Class members' PII and PHI, Defendants implicitly represented that their data security processes were sufficient to reasonably safeguard the PII. This constituted a negligent misrepresentation.

162. Defendants failed to exercise reasonable care or competence in communicating their omissions and misrepresentations.

163. As a direct and proximate result of Defendants' omissions and misrepresentations, Plaintiff and the Class members suffered the various types of damages alleged herein.

164. Plaintiff and the Class members are entitled to all forms of monetary compensation and injunctive relief set forth herein.

Count 5
Unjust Enrichment
On behalf of Plaintiff and the Nationwide Class Against All Defendants

165. Plaintiff incorporates by reference and realleges each and every allegation above as though fully set forth herein.

166. Plaintiff and the Class members conferred a benefit upon Defendants. Specifically, they provided their PII and PHI to Defendants.

167. In exchange for providing PII and PHI to Defendants, Plaintiff and the Class Members should have received adequate safeguarding of their information.

168. Under principles of equity and good conscience, Defendants should not be permitted to retain the full monetary benefit of their transactions with Plaintiff and the Class members, because Defendants failed to adequately secure consumers' PII and PHI and, therefore, did not provide the full services that consumers transacted for.

169. Defendants acquired consumers' PII and PHI through inequitable means in that they failed to disclose their inadequate data security practices when entering into transactions with patients and obtaining their PII and PHI.

170. If Plaintiff and the Class members would have known that Defendants employed inadequate data security safeguards, they would not have agreed to transact with Defendants.

171. Plaintiff and the Class members have no adequate remedy at law.

172. Defendants continue to retain Class members' PII and PHI while exposing the PII and PHI to a risk of future data breaches. Defendants also continue to derive a financial benefit from using Plaintiff's and the Class members' PII and PHI.

173. As a direct and proximate result of Defendants' conduct, Plaintiff and the Class members have suffered the various types of damages alleged herein.

174. Defendants should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and the Class members, the proceeds that they unjustly derived.

Count 6
Breach of Implied Contract
On behalf of Plaintiff and the Nationwide Class Against All Defendants

175. Plaintiff incorporates by reference and realleges each and every allegation above as though fully set forth herein.

176. Plaintiff and the Class members entered into an implied contract with Defendants when they obtained products or services from Defendants or otherwise provided PII and PHI to Defendants.

177. As part of these transactions, Defendants agreed to safeguard and protect the PII and PHI of Plaintiff and the Class members and to timely and accurately notify them if their PII or PHI was breached or compromised.

178. Plaintiff and the Class members entered into the implied contracts with the reasonable expectation that Defendants' data security practices and policies were reasonable and consistent with legal requirements and industry standards.

179. Plaintiff and the Class members believed that Defendants would use part of the monies paid to Defendants under the implied contracts or the monies obtained from the benefits derived from the PII and PHI they provided to fund proper and reasonable data security practices.

180. Plaintiff and the Class members would not have provided and entrusted their PII and PHI to Defendants or would have paid less for Defendants products or services in the absence of the implied contract or implied terms between them and Defendants.

181. The safeguarding of the PII and PHI of Plaintiff and the Class members was critical to realize the intent of the parties.

182. Plaintiff and the Class members fully performed their obligations under the implied contracts with Defendants.

183. Defendants breached their implied contracts with Plaintiff and the Class members to protect their PII and PHI when they (1) failed to take reasonable steps to use safe and secure systems to protect that information; and (2) disclosed that information to unauthorized third parties.

184. As a direct and proximate result of Defendants' breach of implied contract, Plaintiff and the Class members have been injured and are entitled to damages in an amount to be proven at trial.

185. Such injuries include one or more of the following: ongoing, imminent, certainly impending threat of identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; loss of the value of their privacy and the confidentiality of the stolen PII and PHI; illegal sale of the compromised PII and PHI on the black market; mitigation expenses and time spent on credit monitoring, identity theft insurance, and credit freezes and unfreezes; time spent in response to the Data Breach reviewing bank statements, credit card statements, and credit reports, among other related activities; expenses and time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; lost value of the PII and PHI; the amount of the actuarial present value of ongoing high-quality identity defense and credit monitoring services made necessary as mitigation measures because of the Data Breach; lost benefits of their bargains and overcharges for services or products; nominal and general damages; and other economic and non-economic harm.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of herself and the Class and Subclass set forth herein, respectfully requests the following relief:

A. That the Court certify this action as a class action and appoint Plaintiff and her counsel to represent the Class and Subclass;

B. That the Court grant permanent injunctive relief to prohibit Defendants from continuing to engage in the unlawful acts, omissions, and practices described herein and directing Defendants to adequately safeguard the PII and PHI of Plaintiff and the Class and Subclass by implementing improved security controls;

C. That the Court award compensatory, consequential, and general damages, including nominal damages as appropriate, as allowed by law in an amount to be determined at trial;

D. That the Court award statutory or punitive damages as allowed by law in an amount to be determined at trial;

E. That the Court order disgorgement and restitution of all earnings, profits, compensation, and benefits received by Defendants as a result of Defendants' unlawful acts, omissions, and practices;

F. That the Court award to Plaintiff and the Class and Subclass members the costs and disbursements of the action, along with reasonable attorneys' fees, costs, and expenses; and

G. That the Court award pre- and post-judgment interest at the maximum legal rate and all such other relief as it deems just and proper.

///

///

///

///

///

DEMAND FOR JURY TRIAL

Plaintiff hereby demands a jury trial on all claims so triable.

Dated: January 16, 2024

MUCKLEROY LUNT, LLC

MARTIN A. MUCKLEROY (martin@muckleroylunt.com)
Nevada Bar No. 009634
6077 S. Fort Apache Road, Suite 140
Las Vegas, NV 89148
Tel: (702) 907-0097
Fax: (702) 938-4065

SCHUBERT JONCKHEER & KOLBE LLP
AMBER L. SCHUBERT (aschubert@sjk.law)
2001 Union Street, Suite 200
San Francisco, CA 94123
Tel: (415) 788-4220
Fax: (415) 788-0161

Counsel for Plaintiff and the Proposed Class and Subclass