

1 MARTIN A. MUCKLEROY (martin@muckleroylunt.com)  
2 MUCKLEROY LUNT, LLC  
3 Nevada Bar No. 009634  
4 6077 S. Fort Apache Road, Suite 140  
5 Las Vegas, NV 89148  
6 Tel: (702) 907-0097  
7 Fax: (702) 938-4065

8 AMBER L. SCHUBERT (aschubert@sjk.law) (*pro hac vice* forthcoming)  
9 SCHUBERT JONCKHEER & KOLBE LLP  
10 2001 Union Street, Suite 200  
11 San Francisco, CA 94123  
12 Tel: (415) 788-4220  
13 Fax: (415) 788-0161

14 *Counsel for Plaintiff*

15 **UNITED STATES DISTRICT COURT**  
16 **DISTRICT OF NEVADA**

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

19 Plaintiff,

20 v.

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

24 Defendants.

No.

**CLASS ACTION COMPLAINT**

**JURY TRIAL DEMANDED**

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

4 **INTRODUCTION**

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

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

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

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

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

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

26 7. Plaintiff, individually and on behalf of all others similarly situated, asks the Court  
27 to compel Defendants to adopt reasonable information security practices to secure the sensitive  
28

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

3 **PARTIES**

4 ***Plaintiff***

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

9 ***Defendants***

10 9. Defendant PJ&A is a Nevada corporation with its principal place of business at  
11 1489 W. Warm Springs Road, Henderson, NV 89014. PJ&A provides transcription services to  
12 health care organizations and physicians for dictating and transcribing patient notes. PJ&A is a  
13 citizen of Nevada.

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

17 **JURISDICTION AND VENUE**

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

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

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

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

8 **SUBSTANTIVE ALLEGATIONS**

9 **I. The Data Breach.**

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

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

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

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

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

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

24 21. Another disclosure concerning the Data Breach by PJ&A and posted on Mercy  
25 Health’s website stated that for “some individuals, however, the impacted data may have also  
26 included Social Security numbers, insurance information and clinical information from medical  
27  
28

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

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

5 **II. Defendants Had a Duty to Secure Plaintiff’s Information.**

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

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

11 25. Defendants are covered under the Health Insurance Portability and Accountability  
12 Act (“HIPAA”).

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

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

24 28. HIPAA limits the permissible uses of “protected health information” and prohibits  
25 unauthorized disclosures of “protected health information.”

26 29. HIPAA requires that Defendants implement appropriate safeguards for this  
27 information.  
28

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

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

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

13           33.     HIPAA requires covered entities to have and apply appropriate sanctions against  
14 members of its workforce who fail to comply with the privacy policies and procedures of the  
15 covered entity or the requirements of 45 C.F.R. Part 164, Subparts D or E. *See* 45 C.F.R. §  
16 164.530(e).

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

21           35.     HIPAA also requires the Office of Civil Rights (“OCR”), within the Department  
22 of Health and Human Services (“HHS”), to issue annual guidance documents on the provisions  
23 in the HIPAA Security Rule. *See* 45 C.F.R. §§ 164.302-164.318. For example, “HHS has  
24 developed guidance and tools to assist HIPAA covered entities in identifying and implementing  
25 the most cost effective and appropriate administrative, physical, and technical safeguards to  
26 protect the confidentiality, integrity, and availability of e-PHI and comply with the risk analysis  
27 requirements of the Security Rule.” *See* US Department of Health & Human Services, Security  
28

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

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

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

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

18 **III. Defendants Failed to Comply with Reasonable Cybersecurity Standards.**

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

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

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

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

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

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

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

17           46.     The FTC also recommends that businesses limit access to sensitive information,  
18 require complex passwords to be used on the networks, use industry-tested methods for security,  
19 monitor for suspicious activity on the network, and verify that third-party service providers have  
20 implemented reasonable security measures—a step that would have been particularly prudent in  
21 light of the methods used by the perpetrators in this case.

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

24  
25  
26  
27 <sup>1</sup> [https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-](https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business)  
28 [business](https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business).



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

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

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

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

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

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

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

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

27 \_\_\_\_\_  
28 <sup>2</sup> <https://nvlpubs.nist.gov/nistpubs/cswp/nist.cswp.04162018.pdf>.

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

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

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

15 58. Social Security numbers are among the worst kind of personal information to have  
16 stolen because they may be put to a variety of fraudulent uses and are difficult to change. The  
17 Social Security Administration stresses that the loss of an individual's Social Security number  
18 can lead to identity theft and extensive financial fraud:

19 Identity theft is one of the fastest growing crimes in America. A dishonest person  
20 who has your Social Security number can use it to get other personal information  
21 about you. Identity thieves can use your number and your good credit to apply for  
22 more credit in your name. Then, when they use the credit cards and don't pay the  
23 bills, it damages your credit. You may not find out that someone is using your  
24 number until you're turned down for credit, or you begin to get calls from unknown  
25 creditors demanding payment for items you never bought.

26 Someone illegally using your Social Security number and assuming your identity  
27 can cause a lot of problems.<sup>5</sup>

28 <sup>3</sup> <https://www.marylandattorneygeneral.gov/ID%20Theft%20Documents/Identitytheft.pdf>.

<sup>4</sup> <https://bjs.ojp.gov/content/pub/pdf/vit14.pdf>.

<sup>5</sup> <https://www.ssa.gov/pubs/EN-05-10064.pdf>.

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

6           **IV.     Defendants Failed to Provide Proper Notice.**

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

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

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

25           **V.     Plaintiff’s Experiences.**

26           63.     In the course of her treatment at one or more Mercy Health facilities, Plaintiff  
27 provided her sensitive PII and PHI to Mercy Health.  
28

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

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

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

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

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

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

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

26 \_\_\_\_\_  
27 <sup>6</sup> *Your Personal Data Is for Sale on the Dark Web. Here’s How Much It Costs*, DIGITAL TRENDS  
28 (Oct. 16, 2019), <https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs>.

1 considerable. Indeed, studies confirm that “when privacy information is made more salient and  
2 accessible, some consumers are willing to pay a premium to purchase from privacy protective  
3 websites.”<sup>7</sup>

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

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

15 72. All-inclusive health insurance dossiers containing sensitive health insurance  
16 information, names, addresses, telephone numbers, email addresses, Social Security numbers, and  
17 bank account information, complete with account and routing numbers, can fetch up to \$1,200 to  
18 \$1,300 each on the black market.<sup>9</sup> According to a report released by the Federal Bureau of  
19 Investigation’s (“FBI”) Cyber Division, criminals can sell healthcare records for 50 times the  
20 price of a stolen Social Security or credit card number.<sup>10</sup>

21 \_\_\_\_\_  
22 <sup>7</sup> 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)

23 <https://www.jstor.org/stable/23015560?seq=1>.

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

26 <sup>9</sup> 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](https://www.scmagazine.com/news/breach/health-insurance-credentialsfetch-high-prices-in-the-online-black-market).

27 <sup>10</sup> See Federal Bureau of Investigation, *Health Care Systems and Medical Devices at Risk for*  
28 *Increased Cyber Intrusions for Financial Gain* (Apr. 8, 2014),

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

4 74. Criminals can use stolen PII/PHI to extort a financial payment by “leveraging  
5 details specific to a disease or terminal illness.”<sup>12</sup> Quoting Carbon Black’s Chief Cybersecurity  
6 Officer, one recent article explained: “Traditional criminals understand the power of coercion and  
7 extortion. ... By having healthcare information—specifically, regarding a sexually transmitted  
8 disease or terminal illness—that information can be used to extort or coerce someone to do what  
9 you want them to do.”<sup>13</sup>

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

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

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

20 \_\_\_\_\_  
21 [https://www.illumweb.com/wp-content/uploads/ill-mo-uploads/103/2418/health-](https://www.illumweb.com/wp-content/uploads/ill-mo-uploads/103/2418/health-systemscyber-intrusions.pdf)  
22 [systemscyber- intrusions.pdf](https://www.illumweb.com/wp-content/uploads/ill-mo-uploads/103/2418/health-systemscyber-intrusions.pdf).

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

26 <sup>12</sup> See Andrew Steager, *What Happens to Stolen Healthcare Data*, HEALTHTECH  
27 MAGAZINE (Oct. 20, 2019), [https://healthtechmagazine.net/article/2019/10/what-happens-](https://healthtechmagazine.net/article/2019/10/what-happens-stolen-healthcaredata-perfcon)  
28 [stolen-healthcaredata- perfcon](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.”).

<sup>13</sup> *Id.*

<sup>14</sup> See Federal Trade Commission, *What to Know About Identity Theft*, FED. TRADE  
COMM’N CONSUMER INFO.

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

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

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

8 80. Recent FTC data reveals that identify theft remains the top category of fraud  
9 reports received by the agency.<sup>15</sup> The FTC received over 1,100,000 reports of identity theft in  
10 2022, and over 280,000 for the first quarter of 2023 alone.<sup>16</sup>

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

19 \_\_\_\_\_  
20 <sup>15</sup> FTC Consumer Sentinel Network, Federal Trade Commission,  
21 [https://public.tableau.com/app/profile/federal.trade.commission/viz/FraudandIDTheftMaps/All  
22 ReportsbyState](https://public.tableau.com/app/profile/federal.trade.commission/viz/FraudandIDTheftMaps/AllReportsbyState), (Last visited July 9, 2023).

23 <sup>16</sup> *Id.*

24 <sup>17</sup> The FTC defines identity theft as "a fraud committed or attempted using the identifying  
25 information of another person without authority." 12 C.F.R. § 1022.3(h). The FTC describes  
26 "identifying information" as "any name or number that may be used, alone or in conjunction  
27 with any other information, to identify a specific person," including, among other things,  
28 "[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).

<sup>18</sup> 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-  
can-identity- thieves-do-with-your-personal-information-and-how-can-you-protect-yourself/](https://www.experian.com/blogs/ask-experian/what-can-identity-thieves-do-with-your-personal-information-and-how-can-you-protect-yourself/)  
(last accessed Mar. 21, 2022).

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

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

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

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

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

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

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

<sup>21</sup> *Id.*



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

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

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

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

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

24  
25 <sup>22</sup> 2019 Internet Crime Report Released, FBI, [https://www.fbi.gov/news/stories/2019-internet-  
26 crime-report-released-  
27 021120#:~:text=IC3%20received%20467%2C361%20complaints%20in,%2Ddelivery%20scams  
28 %2C%20and%20extortion](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).

<sup>23</sup> *Id.*

- 1           j. costs associated with time spent and the loss of productivity or the enjoyment
- 2           of one's life from taking time to address and attempt to ameliorate, mitigate,
- 3           and deal with the actual and future consequences of the Data Breach, including
- 4           finding fraudulent charges, purchasing credit monitoring and identity theft
- 5           protection services, and the stress, nuisance, and annoyance of dealing with all
- 6           issues resulting from the Data Breach;
- 7           k. the imminent and certainly impending injury flowing from potential fraud and
- 8           identify theft posed by their PII/PHI being placed in the hands of criminals and
- 9           already misused via the sale of Plaintiff and the Class members' information
- 10           on the Internet black market; and
- 11           l. damages to and diminution in value of their PII/PHI entrusted to Defendants.

12           89. In addition to a remedy for economic harm, Plaintiff and the Class members

13 maintain an interest in ensuring that their PII/PHI is secure, remains secure, and is not subject to

14 further misappropriation and theft.

15           90. Defendants disregarded the rights of Plaintiff and the Class members by (i)

16 intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable

17 measures to ensure that their network servers were protected against unauthorized intrusions; (ii)

18 failing to disclose that Defendants did not have adequately robust security protocols and training

19 practices in place to adequately safeguard Plaintiff and the Class members' PII/PHI; (iii) failing

20 to take standard and reasonably available steps to prevent the Data Breach; and (iv) failing to

21 provide Plaintiff and the Class members prompt notice of the Data Breach.

22           91. The actual and adverse effects to Plaintiff and the Class members, including the

23 imminent, immediate and continuing increased risk of harm for identity theft, identity fraud, and

24 medical fraud directly or proximately caused by Defendants' wrongful actions or inaction and the

25 resulting Data Breach require Plaintiff and the Class members to take affirmative acts to recover

26 their peace of mind and personal security including, without limitation, purchasing credit

27 reporting services, purchasing credit monitoring and/or internet monitoring services, frequently

28

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

5 **CLASS ACTION ALLEGATIONS**

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

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

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

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

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

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

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

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

- 6           a. Whether Defendants knew or should have known that their systems were  
7           vulnerable to unauthorized access;
- 8           b. Whether Defendants failed to take adequate and reasonable measures to ensure  
9           their data systems were protected;
- 10          c. Whether Defendants failed to take available steps to prevent and stop the  
11          breach from happening;
- 12          d. Whether Defendants owed a legal duty to Plaintiff and Class and Subclass  
13          members to protect their PII and PHI;
- 14          e. Whether Defendants breached any duty to protect the personal information of  
15          Plaintiff and Class and Subclass members by failing to exercise due care in  
16          protecting their PII and PHI;
- 17          f. Whether Plaintiff and Class and Subclass members are entitled to actual,  
18          statutory, or other forms of damages and other monetary relief; and,
- 19          g. Whether Plaintiff and Class and Subclass members are entitled to equitable  
20          relief, including injunctive relief or restitution.

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

24           99.     **Adequacy of Representation.** Plaintiff is an adequate Nationwide Class and  
25 Subclass representative because she is a Nationwide Class and Subclass member, and her interests  
26 do not conflict with the Nationwide Class or Subclass’ interests. Plaintiff retained counsel who  
27 are competent and experienced in class action and data breach litigation. Plaintiff and her counsel  
28

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

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

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

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

24 **CLAIMS FOR RELIEF**

25 **Count 1**

26 **Violation of the Ohio Consumer Sales Practices Act**  
27 **On behalf of Plaintiff and the Ohio Subclass Against All Defendants**

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

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

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

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

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

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

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

23           110. Defendants’ unfair, deceptive, and unconscionable acts and practices include: (a)  
24 failing to implement and maintain reasonable security and privacy measures to protect Plaintiff’s  
25 information, which was a direct and proximate cause of the Data Breach; (b) failing to identify  
26 and remediate foreseeable security and privacy risks and sufficiently improve security and privacy  
27 measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate  
28

1 cause of the Data Breach; (c) failing to comply with common law and statutory duties pertaining  
2 to the security and privacy of Plaintiff's PII and PHI, including duties imposed by the FTC Act,  
3 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach; (d) misrepresenting  
4 that it would protect the privacy and confidentiality of Plaintiff's PII and PHI, including by  
5 implementing and maintaining reasonable security measures; (e) misrepresenting that it would  
6 comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's  
7 PII and PHI, including duties imposed by the FTC Act, 15 U.S.C. § 45; (f) omitting, suppressing,  
8 and concealing the material fact that it did not properly secure Plaintiff's PII and PHI; and (g)  
9 omitting, suppressing, and concealing the material fact that it did not comply with common law  
10 and statutory duties pertaining to the security and privacy of Plaintiff's PII and PHI, including  
11 duties imposed by the FTC Act, 15 U.S.C. § 45.

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

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

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

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

21 115. As a direct and proximate result of Defendants' unfair, deceptive, and  
22 unconscionable acts and practices, Plaintiff has suffered and will continue to suffer injury,  
23 ascertainable losses of money or property, and monetary and non-monetary damages, as alleged  
24 herein, including but not limited to fraud and identity theft; time and expenses related to  
25 monitoring her financial accounts for fraudulent activity; an increased, imminent risk of fraud and  
26 identity theft; loss of value of her PII and PHI; overpayment for Defendants' services; loss of the  
27  
28

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

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

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

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

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

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

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

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

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

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

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



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

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

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

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

22 128. As a direct and proximate result of Defendants' deceptive trade practices, Plaintiff  
23 and the Ohio Subclass members have suffered and will continue to suffer injury, ascertainable  
24 losses of money or property, and monetary and non-monetary damages, as alleged herein,  
25 including but not limited to fraud and identity theft; time and expenses related to monitoring their  
26 financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft;  
27 loss of value of their PII and PHI; overpayment for Defendants' services; loss of the value of  
28

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

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

6 **Count 3**  
7 **Negligence**  
8 **On behalf of Plaintiff and the Nationwide Class Against All Defendants**

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

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

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

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

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

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

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

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

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

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

- 4 a. Defendants’ exclusive ability (and the Class members’ inability) to ensure that  
5 their systems were sufficient to protect against the foreseeable risk that a data  
6 breach could occur;
- 7 b. Section 5 of the FTC Act, 15 U.S.C. § 45, which prohibits “unfair . . . practices  
8 in or affecting commerce,” including, as interpreted and enforced by the FTC,  
9 failing to adopt reasonable data security measures;
- 10 c. Defendants’ common law duties to adopt reasonable data security measures to  
11 protect PII and PHI and to act as a reasonable and prudent person under the  
12 same or similar circumstances would act; and
- 13 d. State statutes requiring reasonable data security measures, including Nev. Rev.  
14 Stat. § 603A.210, which states that businesses possessing personal information  
15 of Nevada residents “shall implement and maintain reasonable security  
16 measures to protect those records from unauthorized access.”

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

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

24 141. Plaintiff and the Class members were the foreseeable victims of Defendants’  
25 inadequate data security.

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

28

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

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

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

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

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

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

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

23 150. Plaintiff and the Class members are entitled to all forms of monetary compensation  
24 set forth herein, including monetary payments to provide adequate identity protection services.  
25 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**

1  
2  
3 151. Plaintiff incorporates by reference and realleges each and every allegation above  
4 as though fully set forth herein.

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

8 One who fails to disclose to another a fact that he knows may justifiably induce the  
9 other to act or refrain from acting in a business transaction is subject to the same  
10 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.

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

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

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

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

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

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

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

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

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

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

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

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

13 **Count 5**  
14 **Unjust Enrichment**  
15 **On behalf of Plaintiff and the Nationwide Class Against All Defendants**

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

25 179. Plaintiff and the Class members believed that Defendants would use part of the  
26 monies paid to Defendants under the implied contracts or the monies obtained from the benefits  
27 derived from the PII and PHI they provided to fund proper and reasonable data security practices.  
28

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

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

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

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

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

15           185. Such injuries include one or more of the following: ongoing, imminent, certainly  
16 impending threat of identity theft crimes, fraud, and other misuse, resulting in monetary loss and  
17 economic harm; actual identity theft crimes, fraud, and other misuse, resulting in monetary loss  
18 and economic harm; loss of the value of their privacy and the confidentiality of the stolen PII and  
19 PHI; illegal sale of the compromised PII and PHI on the black market; mitigation expenses and  
20 time spent on credit monitoring, identity theft insurance, and credit freezes and unfreezes; time  
21 spent in response to the Data Breach reviewing bank statements, credit card statements, and credit  
22 reports, among other related activities; expenses and time spent initiating fraud alerts; decreased  
23 credit scores and ratings; lost work time; lost value of the PII and PHI; the amount of the actuarial  
24 present value of ongoing high-quality identity defense and credit monitoring services made  
25 necessary as mitigation measures because of the Data Breach; lost benefits of their bargains and  
26 overcharges for services or products; nominal and general damages; and other economic and non-  
27 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*

provided by local rules of court. This form, approved by the Judicial Conference of the United States in September 1974, is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. (SEE INSTRUCTIONS ON NEXT PAGE OF THIS FORM.)

**I. (a) PLAINTIFFS**

Andrea Kay

(b) County of Residence of First Listed Plaintiff Campbell County, KY  
(EXCEPT IN U.S. PLAINTIFF CASES)

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

Martin A. Muckleroy  
6077 S Fort Apache Rd., Ste 140  
Las Vegas, NV 89148

**DEFENDANTS**

Perry Johnson & Associates, Inc. and Bon Secours Mercy Health, Inc., d/b/a Mercy Health

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

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

Attorneys (If Known)

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

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

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

	PTF	DEF		PTF	DEF
Citizen of This State	<input type="checkbox"/> 1	<input type="checkbox"/> 1	Incorporated or Principal Place of Business In This State	<input type="checkbox"/> 4	<input checked="" type="checkbox"/> 4
Citizen of Another State	<input checked="" type="checkbox"/> 2	<input type="checkbox"/> 2	Incorporated and Principal Place of Business In Another State	<input type="checkbox"/> 5	<input type="checkbox"/> 5
Citizen or Subject of a Foreign Country	<input type="checkbox"/> 3	<input type="checkbox"/> 3	Foreign Nation	<input type="checkbox"/> 6	<input type="checkbox"/> 6

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

Click here for: [Nature of Suit Code Descriptions.](#)

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

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

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

**VI. CAUSE OF ACTION**

Cite the U.S. Civil Statute under which you are filing (Do not cite jurisdictional statutes unless diversity):  
 28 U.S.C. § 1332(d)(2)  
 Brief description of cause:  
 Negligence, Negligent Misrepresentation, Unjust Enrichment, and Breach of Implied Contract

**VII. REQUESTED IN COMPLAINT:**

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

**VIII. RELATED CASE(S) IF ANY**

(See instructions): JUDGE Hon. Christina D. Silva DOCKET NUMBER 2:23-cv-01851-CDS-EJY

DATE  
January 16, 2024

SIGNATURE OF ATTORNEY OF RECORD

FOR OFFICE USE ONLY

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

UNITED STATES DISTRICT COURT

for the

District of Nevada

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

Plaintiff(s)

v.

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

Defendant(s)

Civil Action No.

SUMMONS IN A CIVIL ACTION

To: (Defendant's name and address)

PERRY JOHNSON & ASSOCIATES, INC.

A lawsuit has been filed against you.

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

MARTIN A. MUCKLEROY
MUCKLEROY LUNT, LLC
6077 S. FORT APACHE RD., STE. 140
LAS VEGAS, NV 89148

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

CLERK OF COURT

Date:

Signature of Clerk or Deputy Clerk

Civil Action No. \_\_\_\_\_

**PROOF OF SERVICE**

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

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

I personally served the summons on the individual at *(place)* \_\_\_\_\_  
\_\_\_\_\_ on *(date)* \_\_\_\_\_; or

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

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

I returned the summons unexecuted because \_\_\_\_\_; or

Other *(specify)*:

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

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

Date: \_\_\_\_\_

\_\_\_\_\_  
*Server's signature*

\_\_\_\_\_  
*Printed name and title*

\_\_\_\_\_  
*Server's address*

Additional information regarding attempted service, etc:

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

UNITED STATES DISTRICT COURT

for the

District of Nevada

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

Plaintiff(s)

v.

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

Defendant(s)

Civil Action No.

SUMMONS IN A CIVIL ACTION

To: (Defendant's name and address)

BON SECOURS MERCY HEALTH, INC.

A lawsuit has been filed against you.

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

MARTIN A. MUCKLEROY
MUCKLEROY LUNT, LLC
6077 S. FORT APACHE RD., STE. 140
LAS VEGAS, NV 89148

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

CLERK OF COURT

Date:

Signature of Clerk or Deputy Clerk

Civil Action No. \_\_\_\_\_

**PROOF OF SERVICE**

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

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

I personally served the summons on the individual at *(place)* \_\_\_\_\_  
\_\_\_\_\_ on *(date)* \_\_\_\_\_; or

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

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

I returned the summons unexecuted because \_\_\_\_\_; or

Other *(specify)*:

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

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

Date: \_\_\_\_\_

\_\_\_\_\_  
*Server's signature*

\_\_\_\_\_  
*Printed name and title*

\_\_\_\_\_  
*Server's address*

Additional information regarding attempted service, etc: