IN THE CIRCUIT COURT OF THE CITY OF ST. LOUIS
STATE OF MISSOURI

Tiffany Jew and Jessica Simpson, individually and on behalf of all others similarly situated, Plaintiffs, v. BJC Health System, Serve: CSC-Lawyers Incorporating Service Co. 221 Bolivar St. Jefferson City, (Cole Co.) MO 65101 Defendant.	Case No. Division: **JURY TRIAL DEMANDED**

CLASS ACTION PETITION

COME NOW Plaintiffs Tiffany Jew and Jessica Simpson ("Plaintiffs"), individually and on behalf of all others similarly situated (collectively, "Class members"), by and through their attorneys, and bring this Class Action Petition against Defendant BJC Health System ("BJC Healthcare"), and complain and allege upon personal knowledge as to themselves and information and belief as to all other matters.

NATURE OF THE CASE

1. Plaintiffs bring this class action against BJC Healthcare for its failure to secure and safeguard their and other Missouri residents' private and confidential medical information, including names, medical record numbers, account numbers, dates of birth, Social Security numbers, driver's license numbers, and treatment or clinical information, including provider names, visit dates, medications, diagnoses, and testing information ("PHI/PII").

2. As one of the largest nonprofit healthcare organizations in the United States, BJC Healthcare operates fifteen hospitals and multiple community health locations in Missouri and Illinois. In the regular course of business, BJC Healthcare collects and retains its current and former patients' PHI/PII, as well as the PHI/PII of individuals it is or has previously provided other health-related services to.

3. On March 6, 2020, unauthorized individuals gained access to the email accounts of three BJC Healthcare employees and the PHI/PII of Plaintiffs and approximately 287,874 other individuals (the "Data Breach").

4. BJC Healthcare owed a duty to Plaintiffs and Class members to implement and maintain reasonable and adequate security measures to secure, protect, and safeguard their PHI/PII against unauthorized access and disclosure. BJC Healthcare breached that duty by, among other things, failing to implement and maintain reasonable security procedures and practices to protect its patients' PHI/PII from unauthorized access and disclosure.

5. As a result of BJC Healthcare's inadequate security, the Data Breach occurred, and Plaintiffs' and Class members' PHI/PII was accessed and disclosed. This action seeks to remedy these failings. Plaintiffs bring this action on behalf of themselves and all other Missouri residents whose PHI/PII was exposed as a result of the Data Breach occurring on March 6, 2020, and first acknowledged by BJC Healthcare on May 5, 2020.

6. Plaintiffs, on behalf of themselves and other members of the Class, assert claims for negligence, negligence *per se*, breach of implied contract, and violation of the Missouri Merchandising Practices Act, and seek injunctive relief, declaratory relief, monetary damages, statutory damages, punitive damages, and all other relief authorized in equity or by law.

JURISDICTION AND VENUE

7. This Court has jurisdiction over the parties and the subject matter of this action.

8. Venue is proper in the City of St. Louis, pursuant to § 407.025 RSMo., because many of the acts complained of occurred in the City of St. Louis, BJC Healthcare is headquartered in the City of St. Louis, and both of Plaintiffs provided BJC Healthcare with their PHI/PII in connection with receiving heath care at Barnes-Jewish Hospital, a BJC Healthcare hospital located in the City of St. Louis. Further, venue is also proper in this Court pursuant to RSMo. §508.010 because Plaintiffs were first injured in the City of St. Louis, which is where the Data Breach occurred.

PARTIES

9. Plaintiff Tiffany Jew is a Missouri resident. After providing BJC Healthcare with her PHI/PII in connection with receiving healthcare at Barnes-Jewish Hospital—a BJC Healthcare facility—she received a letter from BJC Healthcare dated June 12, 2020, notifying her that her PHI/PII was compromised in the Data Breach. After receiving the letter, she spent a couple of hours on the Internet researching what happened and the possible consequences of the Data Breach. As a result of the Data Breach, she has already spent time monitoring her financial accounts and intends to continue to do so in the future.

10. Plaintiff Jessica Simpson is a Missouri resident. After providing BJC Healthcare with her PHI/PII in connection with receiving healthcare at Barnes-Jewish Hospital—a BJC Healthcare facility—she received a letter from BJC Healthcare dated June 12, 2020, notifying her that her PHI/PII was compromised in the Data Breach. Since learning of the Data Breach, she has spent time communicating with her insurance health company regarding the breach.

11. Defendant BJC HealthCare is a nonprofit health care organization with its principal place of business located at 4901 Forest Park Avenue, City of St. Louis, Missouri 63108. BJC Healthcare operates 15 hospitals and multiple community health locations.

FACTUAL ALLEGATIONS

12. As a healthcare provider operating fifteen hospitals and multiple community health locations in Missouri and Southern Illinois, BJC Healthcare provides inpatient and outpatient care, primary care, community health and wellness, workplace health, home health, community mental health, rehabilitation, long-term care, hospice care and other health-related services to its patients.

13. In the regular course of its business, BJC Healthcare collects and maintains the PHI/PII of its patients, former patients, and other persons who it is currently providing or previously provided health-related services to.

14. Prior to providing healthcare services to its patients, BJC Healthcare requests that its patients provide it with a variety of private and confidential health information, including, but not limited to their name, address, email address, phone number(s), date of birth, age, sex, occupation, employer, marital status, Social Security number, Driver's license number, insurance information, family medical history, a list of all drugs they are currently taking, a list of any drugs they are allergic to, and other information. BJC Healthcare also collects and maintains information regarding its patients' medical histories, doctor's appointments and other medical services received, diagnoses, pharmacy records, clinical records, test results, medical images (x-rays, MRIs, etc.), and other information.

15. BJC Healthcare includes a Joint Notice of Privacy Practices ("Privacy Notice") on their website that encompasses all of the hospitals and medical facilities operated by BJC Healthcare. The Privacy Notice is also given to patients when they are admitted into one of BJC's facilities.[1]

16. The Privacy Notice provides that BJC Healthcare may use or disclose its patients' protected health information without written consent or authorization for a variety of purposes, including: (i) to healthcare providers and other personnel involved in providing care or medical treatment or services; (ii) to bill and receive payment for health services rendered; (iii) "to physicians, medical or other health or business professionals for review, consultation, comparison, and planning" in determining what health services are needed; (iv) "to auditors, accountants, attorneys, government regulators or other consultants to assess and/or ensure our compliance with laws or represent [BJC Healthcare]"; (v) to outside organizations or providers to provide services on its behalf; (vi) after removing direct identifying information, "for research, public health activities or other health care operations (such as business planning); and (vii) for certain activities permitted or required by law, including to public health authorities, heath care oversight agencies, in response to certain requests from law enforcement officials, and in response to subpoenas or court orders.

17. The Privacy Notice states that BJC Healthcare is a health care provider under the Health Insurance Portability and Accountability Act (HIPAA) of 1996.[2]

18. Plaintiffs and Class members are or were patients of BJC Healthcare or received health-related services from BJC Healthcare, and entrusted BJC Healthcare with their PHI/PII.

[1] *See* https://www.bjc.org/For-Patients-Visitors/Patient-Privacy
[2] *See Id.*

19. The storage of Plaintiffs' and Class Members PHI/PII in unencrypted format in the emails of three BJC Healthcare employees was in violation of established industry practices and the Health Insurance Portability and Accountability Act of 1996 ("HIPAA").

The Data Breach

20. On March 6, 2020, an unauthorized individual gained access to the email accounts of three BJC Healthcare employees, compromising the PHI/PII of approximately 287,876 individuals.

21. On May 5, 2020, BJC Healthcare published a *Notice to Patients* on its website stating that the compromised email accounts included:

> some patients' names, dates of birth, medical record or patient account numbers, and limited treatment and/or clinical information, such as visit dates, provider names, medications, diagnoses, and/or testing information. In some instances, patients' Social Security numbers and/or drivers' license numbers were also identified in the accounts.[3]

22. The Data Breach involved compromised PHI/PII from the following BJC Healthcare affiliated hospitals and service organizations:

- Alton Memorial Hospital
- Barnes-Jewish Hospital
- Barnes-Jewish St. Peters Hospital
- BJC Corporate Health Services (dba BarnesCare)
- BJC Medical Group

[3] *See* https://www.bjc.org/Newsroom/Article/ArtMID/5522/ArticleID/4438/Notice-to-Patients.

- Boone Hospital Center
- Christian Hospital
- Missouri Baptist Medical Center
- Missouri Baptist Sullivan Hospital
- Parkland Health Center Farmington
- Parkland Health Center Bonne Terre
- Progress West Hospital
- St. Louis Children's Hospital

23. On or around June 12, 2020, BJC Healthcare sent letters to all persons whose PHI/PII was compromised in the Data Breach.

BJC Healthcare Knew that Criminals Target PHI

24. Prior to and at the time of the Data Breach, BJC Healthcare knew its patients' PHI, including Plaintiffs' and Class members' PHI/PII, was a target for malicious actors. Despite such knowledge, BJC Healthcare failed to implement and maintain reasonable and appropriate security measures to protect Plaintiffs' and Class members' PHI/PII from cyber-attacks BJC Healthcare should have anticipated and guarded against.

25. Between May 9, 2017 and January 23, 2018, the private and confidential patient records—including name, address, telephone number, date of birth, Social Security number, drivers' license number, insurance information, and treatment related information—of 33,420 patients were stored on an unsecure BJC Healthcare server and publicly accessible.

26. BJC Healthcare experienced a second data breach on October 25, 2018, when a hacker uploaded malware onto its patient portal, enabling the hacker to intercept the private and confidential information—names, addresses, birth dates, and credit card details or bank details—

of persons making payment in connection with 5,850 credit/debit card payments between October 25, 2018 and November 8, 2018.

27. Protected health information is a high-value target for identity thieves. In 2014, the FBI informed that "[c]yber actors will likely increase cyber intrusions against healthcare systems" and warned that the "healthcare industry is not technically prepared to combat against cyber criminals' basic cyber intrusion tactics, techniques and procedures[.]"[4]

28. The Identity Theft Resource Center reported that the Medical/Healthcare sector had the second largest number of breaches in 2018 and the highest rate of exposure per breach. According to the ITRC this sector suffered 363 data breaches exposing over 9 million records in 2018.[5] These included Blue Cross Blue Shield of Michigan (15K records exposed), Atrium Health (over 2M records exposed), UnityPoint Health (over 1M records), LifeBridge Health (over 500K), FastHealth Corporation (over 600K records), among others.

29. A person's protected health information and personally identifiable information is a valuable property right.[6] In a Federal Trade Commission ("FTC") roundtable presentation, former Commissioner, Pamela Jones Harbour, underscored this point by observing:

> Most consumers cannot begin to comprehend the types and amount of information collected by businesses, or why their information may be commercially valuable. Data is currency. The larger the data set, the greater potential for analysis – and profit.[7]

[4] *See* https://publicintelligence.net/fbi-health-care-cyber-intrusions/ (FBI, April 8, 2014).
[5] Identity Theft Resource Center, *2018 End-of-Year Data Breach Report, available at* https://www.idtheftcenter.org/wp-content/uploads/2019/02/ITRC_2018-End-of-Year-Aftermath_FINAL_V2_combinedWEB.pdf.
[6] *See* John T. Soma, et al., *Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets*, 15 RICH. J.L. & TECH. 11, at *3-4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).
[7] Federal Trade Commission, *Statement of FTC Commissioner Pamela Jones Harbour* (Remarks Before FTC Exploring Privacy Roundtable) (Dec. 7, 2009), *available at* https://www.ftc.gov/public-statements/2009/12/remarks-ftc-exploring-privacy-roundtable.

30. The value of a person's protected health information and personally identifiable information as a commodity is measurable.[8] "[Personally identifiable information], which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets."[9] It is so valuable to identity thieves that once personally identifiable information or protected health information has been disclosed, criminals often trade it on the "cyber black-market" for several years.

31. Companies recognize personally identifiable information and protected health information as an extremely valuable commodity akin to a form of personal property.

32. As a result of its real value and the recent large-scale data breaches, identity thieves and cyber criminals have openly posted credit card numbers, SSNs, personally identifiable information and other sensitive information directly on various Internet websites making the information publicly available. This information from various breaches, including the information exposed in the Data Breach, can be aggregated and become more valuable to thieves and more damaging to victims. In one study, researchers found hundreds of websites displaying stolen PII and other sensitive information. Strikingly, none of these websites were blocked by Google's safeguard filtering mechanism—the "Safe Browsing list."

[8] *See* Robert Lowes, *Stolen EHR [Electronic Health Record] Charts Sell for $50 Each on Black Market* (April 28, 2014), *available at* http://www.medscape.com/viewarticle/824192.
[9] *See* Soma, *Corporate Privacy Trend, supra*.

33. Protected health information is particularly valuable and has been referred to as a "treasure trove for criminals."[10] A cybercriminal who steals a person's PHI can end up with as many as "seven to ten personal identifying characteristics of an individual."[11]

34. 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.[12] 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.[13]

35. Criminals can use stolen protected health information to extort a financial payment by "leveraging details specific to a disease or terminal illness."[14] 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."[15]

[10] *See* Healthtech Magazine, *What Happens to Stolen Healthcare Data*, https://healthtechmagazine.net/article/2019/10/what-happens-stolen-healthcare-data-perfcon (Oct. 20, 2019) ("*What Happens to Stolen Healthcare Data* Article") (quoting Tom Kellermann, Chief Cybersecurity Officer, Carbon Black, stating "Health information is a treasure trove for criminals.")
[11] *Id.*
[12] Adam Greenberg, *Health Insurance Credentials Fetch High Prices in the Online Black Market* (July 16, 2013), *available at* https://www.scmagazine.com/home/security-news/health-insurance-credentials-fetch-high-prices-in-the-online-black-market/.
[13] Federal Bureau of Investigation, *Health Care Systems and Medical Devices at Risk for Increased Cyber Intrusions for Financial Gain* (April 8, 2014) *available at* https://www.illuminweb.com/wp-content/uploads/ill-mo-uploads/103/2418/health-systems-cyber-intrusions.pdf.
[14] *What Happens to Stolen Healthcare Data* Article.
[15] *Id.*

36. Recognizing the high value consumers place on their personally identifiable information and protected health information, some companies now offer consumers an opportunity to sell this information to advertisers and other third parties. The idea is to give consumers more power and control over the type of information they share—and who ultimately receives that information. By making the transaction transparent, consumers will make a profit from the surrender of their personally identifiable information or protected health information.[16] This business has created a new market for the sale and purchase of this valuable data.[17]

37. Consumers place a high value not only on their personally identifiable information and protected health information but also on the *privacy* of that data. Researchers shed light on how much consumers value their data privacy – and the amount is 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."[18]

38. Given these facts, any company that transacts business with a consumer and then compromises the privacy of consumers' personally identifiable information and protected health information has thus deprived that consumer of the full monetary value of the consumer's transaction with the company.

Theft of PHI/PII Has Grave and Lasting Consequences for Victims

[16] Steve Lohr, *You Want My Personal Data? Reward Me for It*, N.Y. Times (July 16, 2010) *available at* https://www.nytimes.com/2010/07/18/ business/18unboxed.html.
[17] *See* Julia Angwin and Emil Steel, *Web's Hot New Commodity: Privacy*, Wall Street Journal (Feb. 28, 2011) *available at* https://www.wsj.com/articles/ SB10001424052748703529004576160764037920 27.
[18] Janice Y. Tsai et al., *The Effect of Online Privacy Information on Purchasing Behavior, An Experimental Study Information Systems Research* 22(2) 254, 254 (June 2011), *available at* https://www.jstor.org/stable/23015560?seq=1# page_scan_tab_contents.

39. Theft of personally identifiable information and protected health information is serious. The United States Government Accountability Office noted in a June, 2007 report on Data Breaches ("GAO Report") that identity thieves use personally identifiable information to take over existing financial accounts, open new financial accounts, receive government benefits and incur charges and credit in a person's name.[19] As the GAO Report states, this type of identity theft is so harmful because it may take time for the victim to become aware of the theft and can adversely impact the victim's credit rating.

40. In addition, the GAO Report states that victims of identity theft will face "substantial costs and inconveniences repairing damage to their credit records … [and their] good name." According to the FTC, identity theft victims must spend countless hours and large amounts of money repairing the impact to their good name and credit record.[20]

41. Identity thieves use personally identifiable information for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.[21] According to Experian, "[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

[19] *See* http:///www.gao.gov/new.items/d07737.pdf.
[20] *See* FTC Identity Theft Website: https://www.consumer.ftc.gov/features/feature-0014-identity-theft.
[21] The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 16 C.F.R. § 603.2. 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. *Id*.

withdraw funds; obtain a new driver's license or ID; use the victim's information in the event of arrest or court action.[22]

42. The theft of protected health information is even more serious. Data breaches involving protected health information "typically leave[] a trail of falsified information in medical records that can plague victims' medical and financial lives for years."[23] It "is also more difficult to detect, taking almost twice as long as normal identity theft."[24] "A thief may use your name or health insurance numbers to see a doctor, get prescription drugs, file claims with your insurance provider, or get other care. If the thief's health information is mixed with yours, your treatment, insurance and payment records, and credit report may be affected."[25]

43. A report published by the World Privacy Form and presented at the US FTC Workshop on Informational Injury describes what medical identity theft victims may experience:

- Changes to their health care records, most often the addition of falsified information, through improper billing activity or activity by imposters. These changes can affect the healthcare a person receives if the errors are not caught and corrected.
- Significant bills for medical goods and services not sought nor received.
- Issues with insurance, co-pays, and insurance caps.
- Long-term credit problems based on problems with debt collectors reporting debt due to identity theft.
- Serious life consequences resulting from the crime; for example, victims have been falsely accused of being drug users based on falsified entries to their medical files; victims have had their children removed from them due to medical activities

[22] *See* https://www.experian.com/blogs/ask-experian/what-can-identity-thieves-do-with-your-personal-information-and-how-can-you-protect-yourself/.
[23] Pam Dixon, et al., *The Geography of Medical Identity Theft* (Dec. 12, 2017), https://www.ftc.gov/system/files/documents/public_comments/2018/01/00037-142815.pdf.
[24] *See* https://publicintelligence.net/fbi-health-care-cyber-intrusions/ (FBI, April 8, 2014).
[25] *See* Federal Trade Commission, *Medical Identity Theft*, http://www.consumer.ftc.gov/articles/0171-medical-identity-theft.

of the imposter; victims have been denied jobs due to incorrect information placed in their health files due to the crime.

- As a result of improper and/or fraudulent medical debt reporting, victims may not qualify for mortgage or other loans and may experience other financial impacts.

- Phantom medical debt collection based on medical billing or other identity information.

- Sales of medical debt arising from identity theft can perpetuate a victim's debt collection and credit problems, through no fault of their own.

44. A person whose personally identifiable information or protected health information has been compromised may not see any signs of identity theft for years. According to the GAO Report:

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

45. It is within this context that Plaintiffs and other Class members must now live with the knowledge that their PHI/PII is forever in cyberspace and was taken by people willing to use the information for any number of improper purposes and scams, including making the information available for sale on the black-market.

Damages Sustained by Plaintiffs and the Other Class Members

46. Plaintiffs and other Class members have suffered injury and damages, including, but not limited to: (i) an increased risk of identity theft and medical identity theft; (ii) improper disclosure of their PHI/PII, which is now in the hands of criminals; (iii) the value of their time, effort, and money spent mitigating the increased risk of identity theft and medical identity theft; and (iv) deprivation of the value of their PHI/PII, for which there is a well-established national and international market.

47. Plaintiffs and other Class members have suffered and will continue to suffer additional damages based on the opportunity cost and value of time that Plaintiffs and the other Class members have been forced to expend and must expend in the future to monitor their financial accounts, health insurance accounts, and credit files as a result of the Data Breach.

CLASS ALLEGATIONS

48. This action is brought and may be properly maintained as a class action pursuant to Mo. Sup. Ct. R. 52.08, on behalf of a Class defined as follows:

> All Missouri residents whose PHI/PII was accessed by and disclosed to unauthorized persons in the Data Breach.

Excluded from the Class are BJC Healthcare and its affiliates, parents, subsidiaries, employees, officers, agents, and directors, as well as any judicial officer presider over this matter and the members of their immediate families and judicial staff.

49. Certification of Plaintiffs' claims for class-wide treatment is appropriate because Plaintiffs can prove the elements of their claims on a class-wide basis using the same evidence as would be used to prove those elements in individual actions alleging the same claims.

50. The members in the Class are so numerous that joinder of all Class members in a single proceeding would be impracticable. On information and belief, Class members number in the hundreds of thousands. The precise number of Class members and their addresses is presently unknown to Plaintiffs, but may be ascertained from BJC Healthcare's records.

51. Common questions of law and fact exist as to all Class members and predominate over any potential questions affecting only individual Class members. Such common questions of law or fact include, *inter alia*:

a. Whether BJC Healthcare had a duty to implement and maintain reasonable security procedures and practices to protect and secure Plaintiffs' and Class Members' PHI/PII from unauthorized access and disclosure;

b. Whether BJC Healthcare failed to exercise reasonable care to secure and safeguard Plaintiffs' and Class Members' PHI/PII;

c. Whether BJC Healthcare engaged in unlawful or unfair acts or practices in violation of the Missouri Merchandising Practices Act, Mo. Rev. Stat. § 407.010, *et seq.*

d. Whether an implied contract existed between Class members and BJC Healthcare providing that BJC Healthcare would implement and maintain reasonable security measures to protect and secure Class Members' PHI/PII from unauthorized access and disclosure;

e. Whether BJC Healthcare breached its duties to protect Plaintiffs' and Class members' PHI/PII; and

f. Whether Plaintiffs and other members of the Class are entitled to damages, injunctive relief, or other equitable relief, and the measure of such damages and relief.

52. BJC Healthcare engaged in a common course of conduct giving rise to the legal rights sought to be enforced by Plaintiffs, on behalf of themselves and other Class members. Individual questions, if any, pale in comparison, in both quantity and quality, to the numerous common questions that dominate this action.

53. Plaintiffs' claims are typical of the claims of the Class. Plaintiffs, like all proposed members of the Class, had their PHI/PII compromised in the Data Breach. Plaintiffs

and Class members were injured by the same wrongful acts, practices, and omissions committed by BJC Healthcare, as described herein. Plaintiffs' claims therefore arise from the same practices or course of conduct that give rise to the claims of all Class members.

54. Plaintiffs will fairly and adequately protect the interests of the Class members. Plaintiffs are adequate representatives of the Class in that they have no interests adverse to or that conflict with the Class they seek to represent. Plaintiffs have retained counsel with substantial experience and success in the prosecution of complex consumer protection class actions of this nature.

55. A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. The damages and other financial detriment suffered by Plaintiffs and other Class members are relatively small compared to the burden and expense that would be required to individually litigate their claims against BJC Healthcare, so it would be impracticable for Class members to individually seek redress from BJC Healthcare's wrongful conduct. Even if Class members could afford individual litigation, the court system could not. Individualized litigation creates a potential for inconsistent or contradictory judgments, and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court.

CLAIMS

FIRST CAUSE OF ACTION

NEGLIGENCE

56. Plaintiffs reallege and incorporate by reference all preceding paragraphs as if fully set forth herein.

57. BJC Healthcare owed a duty to Plaintiffs and other Class members to exercise reasonable care in safeguarding and protecting their PHI/PII in its possession, custody, or control.

58. BJC Healthcare knew the risks of collecting and storing Plaintiffs' and other Class members' PHI and the importance of maintaining secure systems. BJC Healthcare knew of the many data breaches that targeted healthcare providers in recent years and, as detailed above, was previously the subject of a data breach through which criminals installed malicious malware on certain of its systems.

59. Given the nature of BJC Healthcare's business, the sensitivity and value of the PHI/PII it maintains, and the resources at its disposal, BJC Healthcare should have identified the vulnerabilities to its systems and prevented the Data Breach from occurring.

60. BJC Healthcare breached these duties by failing to exercise reasonable care in safeguarding and protecting Plaintiffs' and Class members' PHI/PII by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems to safeguard and protect personally identifiable information and protected health information entrusted to it—including Plaintiffs' and Class members' PHI/PII.

61. It was reasonably foreseeable to BJC Healthcare that its failure to exercise reasonable care in safeguarding and protecting Plaintiffs' and Class members' PHI/PII by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems

would result in the unauthorized release, disclosure, and dissemination of Plaintiffs' and Class members' PHI/PII to unauthorized individuals.

62. But for BJC Healthcare's negligent or breach of the above-described duties owed to Plaintiffs and Class members, their PHI/PII would not have been compromised.

63. As a result of BJC Healthcare's above-described wrongful actions, inaction, and want of ordinary care that directly and proximately caused the Data Breach, Plaintiffs and other Class members have suffered (and will continue to suffer) economic damages and other injury and actual harm in the form of, *inter alia*: (i) a substantially increased risk of identity theft and medical theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (ii) improper disclosure of their PHI/PII; (iii) breach of the confidentiality of their PHI/PII; (iv) deprivation of the value of their PHI/PII, for which there is a well-established national and international market; and/or (v) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of medical identity theft they face and will continue to face.

64. Plaintiffs' and other Class members' injuries were proximately caused by BJC Healthcare's violations of the duties enumerated above, which was conducted with complete indifference to or a conscious disregard for the safety of others, such that an award of punitive damages is warranted.

SECOND CAUSE OF ACTION

NEGLIGENCE *PER SE*

65. Plaintiffs reallege and incorporate by reference all preceding paragraphs as if fully set forth herein.

66. BJC Healthcare's duties arise from, *inter alia*, the HIPAA Privacy Rule ("Standards for Privacy of Individually Identifiable Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and E, and the HIPAA Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C (collectively, "HIPAA Privacy and Security Rules").

67. BJC Healthcare's duties also arise from Section 5 of the FTC Act ("FTCA"), 15 U.S.C. § 45(a)(1), which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted by the FTC, the unfair act or practice by business, such as BJC Healthcare, of failing to employ reasonable measures to protect and secure personally identifiable information or protected health information.

68. BJC Healthcare violated HIPAA Privacy and Security Rules and Section 5 of the FTCA by failing to use reasonable measures to protect Plaintiffs' and other Class members' PHI/PII and not complying with applicable industry standards. BJC Healthcare's conduct was particularly unreasonable given the fact that it was previously involved in multiple data breaches, the nature and amount of PHI/PII it obtains and stores, and the foreseeable consequences of a data breach involving PHI/PII including, specifically, the substantial damages that would result to Plaintiffs and the other Class members.

69. BJC Healthcare's violation of HIPAA Privacy and Security Rules and Section 5 of the FTCA constitutes negligence *per se*.

70. Plaintiffs and Class members are within the class of persons that HIPAA Privacy and Security Rules and Section 5 of the FTCA were intended to protect.

71. The harm occurring as a result of the Data Breach is the type of harm HIPAA Privacy and Security Rules and Section 5 of the FTCA were intended to guard against. The

FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair practices or deceptive practices, caused the same type of harm that has been suffered by Plaintiffs and other Class members as a result of the Data Brach.

72. It was reasonably foreseeable to BJC Healthcare that its failure to exercise reasonable care in safeguarding and protecting Plaintiffs' and Class members' PHI/PII by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems ,would result in the release, disclosure, and dissemination of Plaintiffs' and Class members' PHI/PII to unauthorized individuals.

73. The injury and harm that Plaintiffs and the other Class members suffered was the direct and proximate result of BJC Healthcare's violations of HIPAA Privacy and Security Rules and Section 5 of the FTCA. Plaintiffs and Class members have suffered (and will continue to suffer) economic damages and other injury and actual harm in the form of, *inter alia*: (i) a substantially increased risk of identity theft and medical theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (ii) improper disclosure of their PHI/PII; (iii) breach of the confidentiality of their PHI/PII; (iv) deprivation of the value of their PHI/PII, for which there is a well-established national and international market; and/or (v) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of medical identity theft they face and will continue to face.

THIRD CAUSE OF ACTION

BREACH OF IMPLIED CONTRACT

74. Plaintiffs reallege and incorporate by reference all preceding paragraphs as if fully set forth herein.

75. In connection with receiving medical treatment or services from BJC Healthcare, Plaintiffs and other Class members entered into implied contracts with BJC Healthcare.

76. Pursuant to these implied contracts, Plaintiffs and Class members paid money to BJC Healthcare, whether directly or through their insurers, and provided BJC Healthcare with their PHI/PII. In exchange, BJC Healthcare agreed, among other things: (1) to provide medical treatment or services to Plaintiffs and Class members at its various locations; (2) to take reasonable measures to protect the security and confidentiality of Plaintiffs' and Class members' PHI/PII; and (3) to protect Plaintiffs' and Class members PHI/PII in compliance with federal and state laws and regulations and industry standards.

77. The protection of PHI/PII was a material term of the implied contracts between Plaintiffs and Class members, on the one hand, and BJC Healthcare, on the other hand. Had Plaintiffs and Class members known that BJC Healthcare would not adequately protect its patients' PHI/PII, they would not have received medical treatment or services from BJC Healthcare.

78. Plaintiffs and Class members performed their obligations under the implied contract when they provided BJC Healthcare with their PHI/PII and paid—directly or through their insurers—for health care treatment and services from BJC Healthcare.

79. BJC Healthcare breached its obligations under its implied contracts with Plaintiffs and Class members in failing to implement and maintain reasonable security measures to protect and secure their PHI/PII and in failing to implement and maintain

security protocols and procedures to protect Plaintiffs' and Class members' PHI/PII in a manner that complies with applicable laws, regulations, and industry standards.

80. BJC Healthcare's breach of its obligations of its implied contracts with Plaintiffs' and Class members directly resulted in the Data Breach.

81. Plaintiffs and other Class members were damaged by BJC Healthcare's breach of implied contracts because: (i) they paid—directly or through their insurers—for data security protection they did not receive; (ii) they face a substantially increased risk of identity theft and medical theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (iii) their PHI/PII was improperly disclosed to unauthorized individuals; (iv) the confidentiality of their PHI/PII has been breached; (v) they were deprived of the value of their PHI/PII, for which there is a well-established national and international market; and/or (vi) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of medical identity theft they face and will continue to face.

FOURTH CAUSE OF ACTION

VIOLATION OF THE MISSOURI MERCHANDISING PRACTICES ACT

(Mo. Ann. Stat. § 407.020, *et seq.* ("MMPA")

82. Plaintiffs reallege and incorporate by reference all preceding paragraphs as if fully set forth herein.

83. BJC Healthcare offered and continues to offer health care services and other health-related services in the State of Missouri.

84. Plaintiffs and other Class members purchased and received health care services or other services from BJC Healthcare for personal, family, or household purposes.

85. BJC Healthcare engaged in unlawful and unfair practices in violation of the MMPA by failing to implement and maintain reasonable security measures to protect and secure their patients' PHI/PII in a manner that complied with applicable laws, regulations, and industry standards.

86. Due to the Data Breach, Plaintiffs and Class members have suffered an ascertainable loss of property in the form of, *inter alia*, their PHI/PII. Further, BJC Healthcare's failure to adopt reasonable practices in protecting and safeguarding its patients' PHI/PII will force Plaintiffs and other Class members to spend time or money to protect against identity theft. Plaintiffs and Class members are now at a higher risk of medical identity theft and other crimes. This harm sufficiently outweighs any justifications or motives for BJC Healthcare's practice of collecting and storing PHI/PII without appropriate and reasonable safeguards to protect such information.

87. As a result of BJC Healthcare's unfair and unlawful acts or practices, Plaintiffs and other Class members have suffered and will continue to suffer actual damages, including identity theft, medical identity theft, improper disclosure of their PHI/PII, breach of confidentiality of their PHI/PII, and/or lost value of their PHI/PII, lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of identity theft and medical identity they face and will continue to face as a result of the Data Breach.

88. Pursuant to RSMo. §407.025, the Court should also award Plaintiffs their reasonable attorneys' fees and punitive damages.

89. Pursuant to RSMo. §407.025, the Court should also order injunctive relief designed to prevent BJC Healthcare from experiencing another data breach by adopting and implementing best data security practices to safeguard PHI/PII and to provide or extend

credit monitoring services and similar services to protect against all types of identity theft and medical identity theft.

DEMAND FOR JURY TRIAL

Plaintiffs demand a trial by jury of all claims in this Class Action Petition so triable.

PRAYER FOR RELIEF

Plaintiffs, individually and on behalf of the other members of the Class, respectfully request that the Court enter judgment in their favor and against BJC Healthcare as follows:

A. Certifying the Class as requested herein, designating Plaintiffs as Class representatives, and appointing undersigned counsel as Class Counsel;

B. Awarding Plaintiffs and the Class appropriate monetary relief, including actual damages, statutory damages, punitive damages, restitution, and disgorgement;

C. Awarding Plaintiffs and the Class equitable, injunctive, and declaratory relief as may be appropriate designed to prevent BJC Healthcare from experiencing another data breach by adopting and implementing best data security practices to safeguard PHI/PII and to provide or extend credit monitoring services and similar services to protect against all types of identity theft and medical identity theft;

D. Awarding Plaintiffs and the Class pre-judgment and post-judgment interest to the maximum extent allowable;

E. Awarding Plaintiffs and the Class reasonable attorneys' fees, costs, and expenses, as allowable; and

F. Awarding Plaintiffs and the Class such other favorable relief as allowable under law or at equity.

Respectfully submitted,

/s/ John S. Steward_____
John S. Steward #45932
Steward Law Firm, LLC
14824 West Clayton Road, Suite 24
Chesterfield, Missouri 63017
(314) 504-0979
Fax: 314-594-5950
js@molawgroup.com

Alexander Wolff #64247
Wolff & Wolff
1034 S. Brentwood Blvd., Ste. 1900
St. Louis, Missouri 63117
Tel: 314.461.1702
Fax: 314.552.1702
Alex@wolfftriallawyers.com

Of Counsel (PHVs to be submitted):

Ben Barnow
Erich P. Schork
Anthony L. Parkhill
Barnow and Associates, P.C.
205 West Randolph Street, Ste. 1630
Chicago, IL 60606
Tel: 312.621.2000
Fax: 312.641.5504
b.barnow@barnowlaw.com
e.schork@barnowlaw.com
aparkhill@barnowlaw.com