COMMONWEALTH OF KENTUCKY
WARREN CIRCUIT COURT, DIVISION _____
CIVIL ACTION NO. 17-CI-_____

SAMUEL PALMER, on behalf of himself and other persons similarly situated, **Plaintiff,** **v.** **BOWLING GREEN-WARREN COUNTY COMMUNITY HOSPITAL CORPORATION D/B/A MED CENTER HEALTH AND COMMONWEALTH HEALTH CORPORATION, INC.,** **Defendants.**	Civil Action **CLASS-ACTION COMPLAINT, DESIGNATION OF TRIAL COUNSEL AND DEMAND FOR JURY TRIAL**

CLASS ACTION COMPLAINT

Plaintiff, Samuel Palmer, ("Plaintiff"), on behalf of himself and others similarly situated, individually and as class representative, upon information and belief, except for the allegations concerning Plaintiff's own actions, says as follows:

INTRODUCTION

1. This is a class-action Complaint brought by Plaintiff, Samuel Palmer ("Plaintiff") on his own behalf and on behalf of all others similarly situated against Defendants Bowling Green-Warren County Community Hospital Corporation d/b/a Med Center Health ("MCH") and Commonwealth Health Corporation, Inc. ("CHC"), to obtain injunctive and monetary relief for a class of individuals against Defendants for their failure to safeguard their clients' Protected Health Information ("PHI") including diagnosis and procedure codes, and Personal Identifying Information ("PII") including social security numbers, health insurance information, names, and

addresses, which Defendants collected from Plaintiff and Class Members (collectively "Private Information"), and for failing to provide timely, accurate and adequate notice to Plaintiff and other Class Members that their Private Information had been stolen and failing to provide timely, accurate and adequate notice of precisely what types of information were stolen.

PARTIES

2. Plaintiff is an adult individual residing in Butler County, Kentucky.

3. Defendant MCH is a business entity incorporated under the laws of Kentucky with a principal office located at 1101 College Street, Bowling Green, Kentucky. Defendant operates medical facilities in Southcentral Kentucky.

4. Defendant CHC is a business entity incorporated under the laws of Kentucky with a principal office located at 1101 College Street, Bowling Green, Kentucky. CHC is the parent corporation of MCH.

JURISDICTION AND VENUE

5. This Court has jurisdiction over all causes of action asserted herein pursuant to the Kentucky Constitution, § 109, because this case is a cause not given by statute to other trial courts.

6. Venue is proper in this Court because Defendants do business in Warren County and the events in controversy occurred in Warren County.

FACTUAL ALLEGATIONS

A. MCH's Data Breach

7. Defendants are not for profit corporations in the business of providing health care to consumers in Southcentral Kentucky.

8. Defendant MCH "represents the most trusted, full-service healthcare provider" in Southcentral Kentucky.[1]

9. Defendants are "the most highly recognized healthcare in the region."[2]

10. Plaintiff and his family have received health care related services from Defendants on multiple occasions for more than the past decade.

11. Despite storing sensitive Private Information that they knew or should have known was valuable to and vulnerable to criminals, Defendants failed to take adequate measures that could have protected patients' Private Information.

12. On or about March 24, 2017, Defendants announced that in August 2014 and February 2015, an employee of Defendants obtained the Personal Information of approximately 160,000 patients without authorization for any work-related reason (the "Data Breach"). The employee used this information for an outside business interest.

13. Plaintiff received a letter from Defendants dated March 24, 2017 that informed him that Med Center Health "recently uncovered evidence indicating a former employee misused billing information." On January 4, 2017, Defendants found "during the course of an internal investigation" that a former employee obtained billing information on two separate occasions." Specifically, "that in August 2014 and February 2015 the individual in question obtained patient information on an encrypted CD and encrypted USB drive, without any work-related reason to do so." (*See* attached Exhibit A.) Other members of Plaintiff's family also received letters informing them about the breach.

[1] http://www.chc.net/about_us/med_center_health.aspx, last visited April 21, 2017.
[2] *Id*.

14. The letter from Defendants also informed Plaintiff that "[t]he billing information included your name, address, Social Security number, health insurance information, diagnosis and procedure codes and charges for your medical services."

15. Over the past three years, Plaintiff's Personal Information has been fraudulently used. He has received notices from two car dealerships about pending loans in his name for vehicles, including a $50,000 Mercedes. Plaintiff has had to spend time responding to these inquiries and reporting these incidents to the Sheriff's office.

16. In order to protect himself from the fall out of the Data Breach, Plaintiff has spent time and effort to monitor for the theft of his identity. This will continue indefinitely and is the direct and proximate result of Defendants' failure to protect his PHI.

B. Consumers Rely on Defendants' Private Information Security Practices

17. Defendants maintain a Notice of Privacy Practices on their website ("Privacy Practices") which provides in relevant part:

> This Notice of Privacy Practices applies to Med Center Health and all hospitals, physician practices, and clinics operated by Med Center Health in the Bowline Green, Horse Cave, Munfordville, Albany, Franklin, and Scottsville areas.
>
> Our Responsibilities
>
> - We are required by law to maintain the privacy and security of your protected health information.
> - We will let you know promptly if a breach occurs that may have compromised the privacy or security of your information.
> - We must follow the duties and privacy practices described in this notice and give you a copy of it.

- We will not use or share your information other than as described here unless you tell us we can in writing.[3]

18. Thus, Defendants collect and store massive amounts of PII in addition to PHI on their servers and utilizes this information to maximize its profits.

19. Consumers place value in data privacy and security, and they consider it when making decisions about where to receive health care services. Plaintiff would not have utilized Defendants' health care services had he known that Defendants did not take all necessary precautions to secure the personal data given to them by consumers.

20. Defendants failed to disclose their negligent and insufficient data security practices and consumers relied on or were misled by this omission into using Defendants' services.

21. The technology and medical industry is rife with similar examples of hackers targeting users' Private Information, including the hacks of Anthem[4], Premera[5], and St. Joseph Health System[6] among others, all of which predate the time-frame Defendants have identified regarding the Data Breach at issue in the present lawsuit. Moreover, the United States Department of Health and Human Services which maintains a website listing breaches of PHI affecting more than 500 or more individuals, and the list reports more than 1800 breaches since 2009. Here, Defendant not only heard the bell warning of a breach, it rang over and over again,

[3] http://www.chc.net/sites/chc_net/Uploads/files/Footer/HIPAA%20privacy%20update-2017.pdf, last visited April 24, 2017.

[4] Los Angeles Times, *Anthem is warning consumers about its huge data breach. Here's a translation*, March 6, 2015. Available at http://www.latimes.com/business/la-fi-mh-anthem-is-warning-consumers-20150306-column.html, last accessed April 24, 2017.

[5] New York Times, *Premera Blue Cross Says Data Breach Exposed Medical Data*, March 17, 2015. Available at http://www.nytimes.com/2015/03/18/business/premera-blue-cross-says-data-breach-exposed-medical-data.html?_r=0, last accessed April 24, 2017.

[6] Napa Valley Register, *St. Joseph Health System sued for patient data breach*, April 9, 2012. Available at http://napavalleyregister.com/news/local/st-joseph-health-system-sued-for-patient-data-breach/article_948c0896-82a3-11e1-bed6-0019bb2963f4.html, last accessed April 24, 2017.

but Defendant chose to ignore the need for highlighted cyber security to maintain its profit margin.[7]

22. As early as 2014 the FBI alerted healthcare firms that they were the target of hackers, stating "The FBI has observed malicious actors targeting healthcare related systems, perhaps for the purpose of obtaining Protected Healthcare Information (PHI) and/or Personally Identifiable Information (PII)".[8]

C. Stolen Private Information Is Valuable to Hackers and Thieves

23. It is well known and the subject of many media reports that Private Information is highly coveted and a frequent target of hackers. This information is targeted not only for identity theft purposes, but also for committing healthcare fraud, including obtaining medical services under another's insurance. A study by Experian found that the "average total cost" of medical identity theft is "about $20,000" per incident, and that a majority of victims of medical identity theft were forced to pay out-of-pocket costs for healthcare they did not receive in order to restore coverage.[9] Despite well publicized litigation and frequent public announcements of data breaches by medical and technology companies, Defendants opted to maintain an insufficient and inadequate system to protect the PHI and PII of Plaintiff and Class Members.

24. Legitimate organizations and the criminal underground alike recognize the value of PII. Otherwise, they wouldn't aggressively seek or pay for it. For example, in "one of 2013's largest breaches . . . not only did hackers compromise the [card holder data] of three million

[7] Available at https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf, last visited April 24, 2017.
[8] Reuters, *FBI warns healthcare firms they are targeted by hackers*, August 20, 2014. Available at http://www.reuters.com/article/us-cybersecurity-healthcare-fbi_idUSKBN0GK24U20140820, last accessed April 24, 2017.
[9] Elinor Mills, *Study: Medical identity theft is costly for victims*, March 3, 2010, 5:00am PST. Available at: https://www.cnet.com/news/study-medical-identity-theft-is-costly-for-victims/, last accessed April 24, 2017.

users, they also took registration data from 38 million users."[10] Similarly, in the Target data breach, in addition to PCI data pertaining to 40,000 credit and debit cards, hackers stole PII pertaining to 70,000 users.

25. Biographical data is also highly sought after by data thieves. "Increasingly, criminals are using biographical data gained from multiple sources to perpetrate more and larger thefts." *Id.* PII data has been stolen and sold by the criminal underground on many occasions in the past, and the accounts of theft and unauthorized access have been the subject of many media reports. One form of identity theft, branded "synthetic identity theft," occurs when thieves create new identities by combining real and fake identifying information and then use those identities to open new accounts. "This is where they'll take your Social Security number, my name and address, someone else's birthday and they will combine them into the equivalent of a bionic person," said Adam Levin, Chairman of IDT911, which helps businesses recover from identity theft. Synthetic identity theft is harder to unravel than traditional identity theft, experts said: "It's tougher than even the toughest identity theft cases to deal with because they can't necessarily peg it to any one person." In fact, the fraud might not be discovered until an account goes to collections and a collection agency researches the Social Security number.

26. Unfortunately, and as is alleged below, despite all of this publicly available knowledge of the continued compromises of Private Information in the hands of third parties, such as health companies, Defendants' approach at maintaining the privacy of the Plaintiff's and the Class Members' PII and PHI was lackadaisical, cavalier, reckless, or at the very least negligent.

[10]Verizon 2014 PCI Compliance Report, Available at http://www.cisco.com/c/dam/en_us/solutions/industries/docs/retail/verizon_pci2014.pdf (hereafter "2014 Verizon Report"), at 54 last visited April 24, 2017.

D. This Data Breach Will Result in Additional Identity Theft and Identity Fraud.

27. Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the Private Identifying Information and Private Health Information maintained on its systems.

28. The ramifications of Defendants' failure to keep Plaintiff's and Class Members' data secure are severe. As explained by the Federal Trade Commission:

> Medical identity theft happens when someone steals your personal information and uses it to commit health care fraud. Medical ID thieves may use your identity to get treatment — even surgery — or to bilk insurers by making fake claims. Repairing damage to your good name and credit record can be difficult enough, but medical ID theft can have other serious consequences. If a scammer gets treatment in your name, that person's health problems could become a part of your medical record. It could affect your ability to get medical care and insurance benefits, and could even affect decisions made by doctors treating you later on. The scammer's unpaid medical debts also could end up on your credit report.[11]

29. As the FTC recognizes, once identity thieves have personal information, "they can drain your bank account, run up your credit cards, open new utility accounts, or get medical treatment on your health insurance."[12]

30. According to Javelin Strategy and Research, "1 in 4 notification recipients became a victim of identity fraud."[13]

[11] Federal Trade Commission, *Medical ID Theft: Health Information for Older People*, available at https://www.consumer.ftc.gov/articles/0326-medical-id-theft-health-information-older-people, last accessed April 24, 2017.
[12] Federal Trade Commission, *Warning Signs of Identity Theft*, available at https://www.consumer.ftc.gov/articles/0271-warning-signs-identity-theft, last accessed April 24, 2017.
[13] See 2013 Identity Fraud Report: Data Breaches Becoming a Treasure Trove for Fraudsters, available at www.javelinstrategy.com/brochure/276, last visited April 24, 2017 (the "2013 Identity Fraud Report").

31. It is incorrect to assume that reimbursing a consumer for a financial loss due to fraud makes that individual whole again. On the contrary, after conducting a study, the Department of Justice's Bureau of Justice Statistics ("BJS") found that "among victims who had personal information used for fraudulent purposes, 29% spent a month or more resolving problems."[14] In fact, the BJS reported, "resolving the problems caused by identity theft [could] take more than a year for some victims." *Id*. at 11.

32. Javelin Strategy and Research reports that losses from identity theft increased to $21 billion in 2013.[15]

33. There may be a time lag between when harm occurs and when it is discovered, and also between when Private Information is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

34. "[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."[16]

35. Plaintiff and Class Members now face years of constant surveillance of their financial, personal and medical records. The Class is incurring and will continue to incur such damages in addition to any fraudulent charges made to their financial accounts or medical insurance, whether or not such charges are ultimately reimbursed by the credit card companies.

---

[14] Victims of Identity Theft, 2012 (Dec. 2013) at 10, *available at* http://www.bjs.gov/content/pub/pdf/vit12.pdf, last accessed April 24, 2017.
[15] *See* 2013 Identity Fraud Report.
[16] GAO, Report to Congressional Requesters, at p.29 (June 2007), *available at* http://www.gao.gov/new.items/d07737.pdf (emphases added) (last visited April 24, 2017).

E. Plaintiff and Class Members Suffered Damages

36. The Data Breach was a direct and proximate result of Defendants' failure to properly safeguard and protect Plaintiff's and Class Members' Private Identifying Information and Private Health Information from unauthorized access, use, and disclosure, as required by various state and federal regulations, industry practices, and the common law, including Defendants' failure to establish and implement appropriate administrative, technical and physical safeguards to ensure the security and confidentiality of Plaintiff's and Class members' Personal Identifying Information and Personal Health Information to protect against reasonably foreseeable threats to the security or integrity of such information.

37. Plaintiff's and Class Members' Personal Identifying Information and Private Health Information is private and sensitive in nature and was left inadequately protected by Defendants. Defendants did not obtain Plaintiff's and Class Members' consent to disclose either their Personal Identifying Information or their Private Health Information to any other person as required by applicable law and industry standards.

38. As a direct and proximate result of Defendants' wrongful action and inaction and the resulting Data Breach, Plaintiff (as addressed above) and Class Members have been placed at an imminent, immediate, and continuing increased risk of harm from identity theft and identity fraud, requiring them to take time and effort to mitigate the actual and potential impact of the Data Breach on their lives by, among other things, placing "freezes" or "alerts" with credit reporting agencies, contacting their health insurance providers, contacting their financial institutions, closing or modifying financial accounts, and closely reviewing and monitoring their medical "explanations of benefits" and credit reports and accounts for unauthorized activity.

39. Defendants' wrongful actions and inaction directly and proximately caused the theft and dissemination into the public domain of Plaintiff's and Class Members' Private Health Information and Personal Identifying Information, causing them to suffer, and continue to suffer, economic damages and other actual harm for which they are entitled to compensation including:

a. Theft of their personal, medical, and/or financial information;

b. The reputational harms suffered by Defendants' publication of private facts in the form of Plaintiff's and Class Members' diagnosis and procedure codes and charges for medical services;

c. The imminent and certainly impending injury flowing from potential fraud and identity theft posed by their personal and medical information being placed in the hands of criminals;

d. The untimely and inadequate notification of the Data Breach;

e. The improper disclosure of Plaintiff's and Class Member's private information;

f. Loss of Privacy;

g. Ascertainable loss in the form of out-of pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach;

h. Ascertainable losses in the form of deprivation of the value of their Personal Identifying Information and Private Health Information, for which there is a well-established national and international market;

i. Overpayments to Defendants for products and services in that a portion of the price paid for such products and services by Plaintiffs and Class

members to Defendants was for the costs of reasonable and adequate safeguards and security measures that would protect users' Private Information, which Defendants did not implement and, as a result, Plaintiff and Class members did not receive what they paid for and were overcharged by Defendants.

CLASS ACTION ALLEGATIONS

40. This action is brought and may properly proceed as a class action, pursuant to the provisions of Rule 23 of the Kentucky Rules of Civil Procedure. Plaintiff brings this action on behalf of himself and all others similarly situated. Plaintiff seeks certification of a Class, initially defined as follows:

> **All persons in Kentucky whose personal information was disclosed in the Data Breach announced by MCH on or about March 24, 2017.**

41. The Class for those whose benefit this action has been brought is so numerous that joinder of all members is impracticable, as Defendants have indicated it believes more than 160,000 individuals may have been impacted in the Breach.

42. Plaintiff's claims are typical of the claims of the members of the Class, since all such claims arise out of Defendants' failure to safeguard user's information and by Defendants' own terms of service every Class Member will be subject to Kentucky law.

43. Plaintiff does not have interests antagonistic to the interests of the Class.

44. The Class, of which Plaintiff is a member, is readily identifiable by reference to Defendants' records.

45. Plaintiff will fairly and adequately protect the interests of the Class and has retained competent counsel experienced in the prosecution of consumer litigation. Proposed Class Counsel has investigated and identified potential claims in the action; has a great deal of

experience in handling class actions, other complex litigation, and claims of the type asserted in this action.

46. There are common questions of law and fact effecting the rights of all class members, including the following:

a. Whether Defendant violated Kentucky law by failing to implement reasonable data security measures;

b. Whether Defendant violated common and statutory law by failing to promptly notify Class Members their Private Health Information and Personal Identifying Information had been compromised;

c. Whether Class Members may obtain injunctive relief against Defendants under Kentucky law to require that it safeguard or destroy, rather than retain as it has, the Private Health Information and Personal Identifying Information of Plaintiff and the Class Members;

d. Which security procedures and which data-breach notification procedure Defendants should be required to implement as part of any injunctive relief ordered by the Court;

e. Whether Defendants have contractual obligations to use reasonable data security measures;

f. Whether Defendants have complied with contractual obligations to use reasonable data security measures;

g. What data security measures, if any, must be implemented by Defendants to comply with its contractual obligations;

h. Whether Defendants have implied contractual obligations to use reasonable data security measures;

i. Whether Defendants have complied with implied contractual obligations to use reasonable data security measures;

j. What data security measures, if any, must be implemented by Defendants to comply with their implied contractual obligations;

k. What the nature of the relief should be, including equitable relief, to which Plaintiff and Class Members are entitled.

47. A class action is superior to other available methods for the fair and efficient adjudication of this controversy since joinder of all members is impracticable. While the economic damages suffered by the individual Class Members are significant, the amount is modest compared to the expense and burden of individual litigation. A class action will cause an orderly and expeditious administration of the claims of the Class and will foster economies of time, effort and expense.

48. The questions of law and/or fact common to the members of the Class predominate over any questions affecting only individual members.

49. The prosecution of separate actions by individual members of the Class would run the risk of inconsistent or varying adjudications, which would establish incompatible standards of conduct for the Defendants in this action or the prosecution of separate actions by individual members of the Class would create the risk that adjudications with respect to individual members of the Class and Subclass would as a practical matter be dispositive of the interests of the other members not parties to the adjudications or substantially impair or impede their ability to protect their interests. Prosecution as a class action will eliminate the possibility of repetitious litigation.

50. Defendants have acted or refused to act on grounds generally applicable to the Class, thereby making appropriate final injunctive relief or corresponding declaratory relief with respect to the class as a whole.

51. Plaintiff does not anticipate any difficulty in the management of this litigation.

COUNT ONE
Negligence
(As to Plaintiff and the Class)

52. Plaintiff repeats and realleges all of the allegations set forth in paragraphs 1-51 as if fully set forth herein.

53. Defendants, through the course of providing services to Plaintiff and the Class, obtained their Private Information.

54. Defendants knew, or should have known, of the risks inherent in collecting and storing the PII and PHI of Plaintiff and Class Members.

55. Upon accepting and storing Plaintiff's and Class Members' PHI and PII in their computer database systems, Defendants undertook and owed a duty to Plaintiff and Class Members to exercise reasonable care to secure and safeguard that information and to utilize commercially reasonable methods to do so. Defendants knew, acknowledged, and agreed that the Plaintiff and Class Member's PHI and PII was private and confidential and would be protected as private and confidential.

56. Defendants breached their duties of care to Plaintiff and Class Members by failing to provide fair, reasonable or adequate computer systems and data security practices to safeguard Plaintiff's PHI and PII.

57. Defendants acted with wanton disregard for the security of Plaintiff and Class Members' PHI and PII. Defendant knew or should have known that it had inadequate computer systems and data security practices to safeguard such information.

58. The law imposed an affirmative duty on Defendants to timely discover and disclose the unauthorized access and theft of the PHI and PII to Plaintiffs and the Class so that Plaintiff and Class Members could take appropriate measures to mitigate damages, protect against adverse consequences, and thwart future misuse of their Private Information.

59. To date, Defendants have not provided sufficient information to Plaintiff and Class Members regarding the extent of the unauthorized access and continues to breach its disclosure obligations to Plaintiff and the Class.

60. Defendants also breached their duty to Plaintiff and the Class Members to adequately protect and safeguard Plaintiff and Class Members' information by knowingly disregarding standard information security principles, despite obvious risks, and by allowing unmonitored and unrestricted access to unsecured Private Information. Furthering its dilatory practices, Defendants failed to provide adequate supervision and oversight of the Private Information with which it is entrusted, in spite of the known risk and foreseeable likelihood of breach and misuse, which permitted a third party to gather Plaintiffs' and Class Members' Private Information, misuse the Private Information, and intentionally disclose it to others without consent.

61. Through Defendants' acts and omissions described in this Complaint, including Defendants' failure to provide adequate security and its failure to protect Plaintiffs' and Class Members' Private Information from being foreseeably captured, accessed, disseminated, stolen, and misused, Defendants unlawfully breached their duty to use reasonable care to adequately

protect and secure Plaintiffs' and Class Members' Private Information during the time it was within Defendants' possession or control.

62. Further, through its failure to timely discover and provide clear notification of the Data Breach to consumers, Defendants prevented Plaintiffs and Class Members from taking meaningful, proactive steps to secure their Private Information.

63. Upon information and belief, Defendants improperly and inadequately safeguarded the Private Information of Plaintiffs and Class Members in deviation from standard industry rules, regulations, and practices at the time of the Data Breach.

64. Defendants' failure to take proper security measures to protect Plaintiff's and Class Members' sensitive Private Information as described in this Complaint, created conditions conducive to a foreseeable, intentional criminal act, namely the unauthorized access of Plaintiff's and Class Members' Private Information.

65. Defendants' conduct was grossly negligent and departed from all reasonable standards of care, including, but not limited to: failing to adequately protect the Private Information; failing to conduct adequate regular security audits; failing to provide adequate and appropriate supervision of persons having access to Plaintiff's and Class Members' Private Information; and failing to provide Plaintiff and Class Members with timely and sufficient notice that their sensitive Private Information had been compromised.

66. Neither Plaintiff nor the other Class Members contributed to the Data Breach and subsequent misuse of their Private Information as described in this Complaint.

67. As a direct and proximate cause of Defendants' conduct, Plaintiff and the Class suffered damages including, but not limited to: damages from identity theft, which may take months, if not years, to discover and detect, given the far-reaching, adverse, and detrimental

consequences of identity theft and loss of privacy. The nature of other forms of economic damage and injury may take years to detect and the potential scope can only be assessed after a thorough investigation of the facts and events surrounding the theft mentioned above.

COUNT TWO
Breach of Contract
(On Behalf of Plaintiff and the Class)

68. Plaintiff repeats and realleges all of the allegations set forth in paragraphs 1-51 as if fully set forth herein.

69. As set forth above, Plaintiff and Class Members received healthcare services from Defendants.

70. As set forth above, the contract between Plaintiff and Class members and Defendants was supported by consideration in many forms including the payment of monies for healthcare services.

71. Plaintiff and Class Members performed pursuant to these contracts, and satisfied all conditions, covenants, obligations, and promises of the agreements.

72. Under the contracts, Defendants were obligated, as outlined in the Privacy Practices, to maintain the confidentiality of Plaintiff's and Class Member's PHI and PII.

73. As a result of Defendants' breach of contract, by failing to adequately secure Plaintiff and Class Member's PHI and PII, Plaintiff and Class members did not receive the full benefit of the bargain, and instead received services that were less valuable than described in the contracts. Plaintiff and Class Members, therefore, were damaged in an amount at least equal to the difference in value between what was promised and what Defendants ultimately provided.

74. Also as a result of Defendants' breach of contract, Plaintiff and Class Members have suffered actual damages resulting from the theft of their PHI and PII, and remain at imminent risk of suffering additional breaches in the future.

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

75. Plaintiff repeats and realleges all of the allegations set forth in paragraphs 1-51 as if fully set forth herein.

76. Plaintiff and Class members were required to provide their Private Information, including names, addresses, Social Security numbers, and other personal information, to Defendants as a condition to receive medical services.

77. Implicit in the agreement between Defendants and their patients was the obligation that both parties would maintain information confidentially and securely.

78. Defendants' Privacy Practices provides that "[w]e are required by law to maintain the privacy and security of your protected health information. . . We will let you know promptly if a breach occurs that may have compromised the privacy or security of your information. . . . We will not use or share your information other than as described here unless you tell us we can in writing."

79. Defendants had an implied duty of good faith to ensure that the Private Information of Plaintiff and Class members in their possession was only used to provide agreed-upon medical services from Defendants.

80. Defendants had an implied duty to reasonably safeguard and protect the Private Information of Plaintiff and Class members from unauthorized disclosure or uses.

81. Additionally, Defendants implicitly promised to retain this Private Information only under conditions that kept such information secure and confidential.

82. Plaintiff and Class members fully performed their obligations under the implied contract with Defendants. Defendants did not.

83. Plaintiff and Class members would not have provided their confidential Private Information to Defendants in the absence of their implied contracts with Defendants, and would have instead retained the opportunity to control their Private Information for uses other than medical services from Defendants.

84. Defendants breached the implied contracts with Plaintiff and Class members by failing to reasonably safeguard and protect Plaintiffs' and Class members' PII, which was compromised as a result of the Data Breach.

85. Defendants' acts and omissions have materially affected the intended purpose of the implied contacts requiring Plaintiff and Class members to provide their Private Information as a condition to receive medical services.

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

placing freezes on credit reports; (vi) the continued risk to their Private Information, which remain in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the Private Information of employees and former employees in its continued possession; and, (vii) future costs in terms of time, effort and money that will be expended to prevent, detect, contest, and repair the impact of the Private Information compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class members.

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

87. Plaintiff repeats and realleges all of the allegations set forth in paragraphs 1-51as if fully set forth herein.

88. Plaintiff and Class Members had a legitimate expectation of privacy to their Private Information and were entitled to the protection of this information against disclosure to unauthorized third parties.

89. Defendants owed a duty to its patients, including Plaintiff and Class Members, to keep their PII and PHI contained as a part thereof, confidential.

90. Defendants intentionally released files containing the PII and PHI of Plaintiff and Class Members to an employee without a legitimate business-related purpose and use.

91. The unauthorized release to, custody of and examination by unauthorized third parties of the Private Information of Plaintiffs and Class Members, especially where the information includes Social Security numbers and health insurance information, would be highly offensive to a reasonable person.

92. The intrusion was into a place or thing, which was private and is entitled to be private. Plaintiff and Class Members disclosed their Private Information to Defendants to receive medical care, but did so privately with an intention that the Private Information would be kept confidential and would be protected from unauthorized disclosure. Plaintiff and Class Members were reasonable to believe that such information would be kept private and would not be disclosed without their authorization.

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

94. As a proximate result of the above acts and omissions of Defendants, the Private Information of Plaintiff and Class Members was disclosed to and used by third parties without authorization, causing Plaintiff and Class Members to suffer damages.

95. Unless and until enjoined, and restrained by order of this Court, Defendants' wrongful conduct will continue to cause great and irreparable injury to Plaintiff and Class Members in that Private Information is still stored and housed on Defendants' computer systems, and, thus, can be viewed, distributed and used by unauthorized persons. Plaintiff and Class Members have no adequate remedy at law for the injuries in that a judgment for monetary damages will not end the invasion of privacy for Plaintiff and the Class.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of all Class Members proposed in this Complaint, prays for judgment as follows:

a. For an Order certifying the Class as defined here, and appointing Plaintiff and

his Counsel to represent the Class;

b. For equitable relief enjoining Defendants from engaging in the wrongful conduct complained of here pertaining to the misuse and/or disclosure of Plaintiff and Class Members' Private Health Information and Personal Identifying Information, and from refusing to issue prompt, complete, and accurate disclosures to the Plaintiff and Class Members;

c. For equitable relief compelling Defendants to utilize appropriate methods and policies with respect to consumer data collection, storage, and safety and to disclose with specificity to Class Members the type of Private Health Information and Personal Identifying Information compromised;

d. For equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendants' wrongful conduct;

e. For an award of actual damages and compensatory damages, in an amount to be determined;

f. For an award of costs of suit and attorneys' fees; and

g. Such other and further relief as this court may deem just and proper.

JURY TRIAL DEMAND

Plaintiff demands a jury trial on all issues so triable.

Dated: May 11, 2017

Respectfully submitted,

/s / *Kelli Lester*

KELLI LESTER
Morgan & Morgan – Bowling Green
360 E. 8th Avenue, Suite 305
Bowling Green, KY 42101
Phone: (270) 495-6801
Email: klester@forthepeople.com

JOHN A. YANCHUNIS*
jyanchunis@ForThePeople.com
MARISA GLASSMAN*
mglassman@ForThePeople.com
MORGAN & MORGAN
COMPLEX LITIGATION GROUP
201 N. Franklin Street, 7th Floor
Tampa, Florida 33602
Telephone: (813) 223-5505
Facsimile: (813) 223-5402

JEAN SUTTON MARTIN*
jean@jsmlawoffice.com
LAW OFFICE OF JEAN SUTTON
MARTIN PLLC
2018 Eastwood Road Suite 225
Wilmington, NC 28403
Telephone: (910) 292-6676
Facsimile: (888) 316-3489

Attorneys for Plaintiff and the Putative Class
* *pro hac vice* application to be submitted