IN THE UNITED STATES DISTRICT COURT
MIDDLE DISTRICT OF FLORIDA
TAMPA DIVISION

RAY STOLL, HEIDI IMHOF, and CHASE WHITMAN on behalf of B.W., a minor child, individually and on behalf of all others similarly situated, Plaintiffs, v. MUSCULOSKELETAL INSTITUTE, CHARTERED d/b/a FLORIDA ORTHOPAEDIC INSTITUTE, Defendant.	Case No.: 8:20-cv-01798-CEH-AAS **AMENDED CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiffs Ray Stoll ("Stoll"), Heid Imhof ("Imhof"), and Chase Whitman, on behalf of B.W., a minor child ("Whitman") (together, "Plaintiffs"), individually and on behalf of the Class defined below of similarly situated persons, bring this Class Action Complaint and allege the following against Defendant Musculoskeletal Institute, Chartered d/b/a Florida Orthopaedic Institute ("FOI" or "Defendant"), based upon personal knowledge with respect to Plaintiffs and on information and belief derived from, among other things, investigation of counsel and review of public documents as to all other matters:

NATURE OF THE ACTION

1. Plaintiffs brings this class action against Defendant for Defendant's failure to properly secure and safeguard protected health information as defined by the Health Insurance Portability and Accountability Act ("HIPAA"), medical

information, and other personally identifiable information, including without limitation names, social security numbers, dates of birth, addresses, diagnosis codes, financial information, and treatment information (collectively, "PII"), for failing to comply with industry standards to protect information systems that contain that PII, and for failing to provide timely, accurate, and adequate notice to Plaintiffs and other Class Members that their PII had been compromised. Plaintiffs seek, among other things, orders requiring Defendant to fully and accurately disclose the nature of the information that has been compromised, to adopt reasonably sufficient security practices and safeguards to prevent incidents like the disclosure in the future, and to provide for the lifetimes of Plaintiffs and Class Members identity theft protective services as Plaintiffs and Class Members will be at an increased risk of identity theft due to the conduct of Defendant as described herein

2. On or about April 9, 2020, FOI experienced a ransomware attack which resulted in exposure of sensitive and private PII of at least 100,000 patients, and potentially in excess of 150,000 patients of Defendant (the "Data Disclosure"). An exemplar of the Notification of Data Security Incident letter from Florida Orthopaedic Institute dated June 18, 2020 and June 19, 2020 (the "Notification Letter") that was sent to Plaintiffs and Class Members is attached hereto as **Exhibit** "**A**."

3. This case involves a *breach* of a computer system *by* a third party, as well as unauthorized *disclosure* of the PII of Plaintiffs and Class Members by the Defendant *to* unknown third parties. As a result of Defendant's failure to implement and follow basic security procedures Plaintiffs' and Class Members' PII is now in the hands of

thieves and unknown criminals. Plaintiffs and Class Members now face a substantial increased risk of identity theft. Consequently, Defendant's current and former customers have had to spend, and will continue to spend, significant time and money in the future to protect themselves due to Defendant's failures.

4. Additionally, as a result of Defendant's failure to follow contractually-agreed upon, federally-prescribed, industry standard security procedures, Plaintiffs and Class Members received only a diminished value of the services Defendant was to provide. Defendant expressly represented that, in compliance with HIPAA, it would "maintain the privacy of [Plaintiffs' and Class Members'] health information," and "obtain [Plaintiffs' and Class Members'] written authorization before disclosing [their] protected health information."[1]

5. Defendant provided an extensive list and description of situations and reasons why Plaintiffs', Class Members', and customers/patients' protected health information and PII might be disclosed to a third party—none of which is the case here.[2]

6. Accordingly, Plaintiffs, individually and on behalf of all others similarly situated, alleges claims negligence, invasion of privacy, breach of implied contract, negligence *per se*, unjust enrichment, breach of fiduciary duty, violation of Florida's Deceptive and Unfair Trade Practices Act (Florida Statute § 501.203, *et seq*.), and breach of confidence.

[1] https://www.floridaortho.com/privacy-policy/
[2] https://www.floridaortho.com/privacy-policy/

JURISDICTION AND VENUE

7. This Court has jurisdiction over this action as Paintiffs seek on their own behalf and Class Members damages in excess of the minimum jurisdictional limits of this Court and equitable relief.

8. This Court has personal jurisdiction over FOI because FOI maintains its principal place of business in this Circuit, regularly conducts business in this Circuit, and is authorized to and does conduct substantial business in this Circuit.

PARTIES

9. Plaintiff Ray Stoll is a citizen and resident of Tampa, Florida.

10. Plaintiff Heidi Imhof is a citizen and resident of Land O' Lakes, Florida.

11. Plaintiff Chase Whitman, on behalf of B.W., a minor child, are both citizens and residents of Mandeville, Louisiana.

12. At all times relevant to this Complaint, Plaintiffs were customers and patients of FOI, whose PII was disclosed without authorization to an unknown third party as a result of the Data Disclosure.

13. Defendant FOI is a Florida corporation with its principal address at 13020 N Telecom Parkway, Temple Terrace, FL 33637-0925, according to its registration with the Florida Secretary of State.

14. Founded in 1989, Defendant has grown from twelve orthopaedists working in one office and one hospital to over forty physicians, twenty-five mid-level providers, fifteen Fellows, and a professional staff of more than 700, working in nine offices and nineteen regional hospitals, two Surgery Centers and two Orthopaedic

Urgent Care centers.

15. FOI offers a comprehensive range of specialized orthopedic services involving, bones, muscles or joints, including foot and ankle, hand and write, joint arthroplasty, oncology, orthopaedic trauma, pain management, rehabilitation medicine, shoulder and elbow, spine surgery and sports medicine.

FACTUAL BACKGROUND

A. Security Breaches Lead to Identity Theft

16. In June 2007, the United States Government Accountability Office reported that identity thieves use identifying data, such as Social Security Numbers, to open financial accounts, intercept government benefits, and incur charges and credit in a person's name.[3] The GAO affirmed this type of identity theft is the most harmful because it may take some time for the victim to become aware of the theft and can adversely impact the victim's credit rating. In addition, the GAO Report informs that victims of identity theft will face "substantial costs and inconveniences repairing damage to their credit records…[and their] good name."[4]

17. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[5] The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to

[3] *Data Breaches are Frequent, but Evidence of Resulting Identity Theft is Limited; However, the Full Extent is Unknown*, GAO (June 2007), *available at* https://www.gao.gov/new.items/d07737.pdf (the "GAO Report")
[4] *Id*.
[5] 17 C.F.R. § 248.201.

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."[6]

18. The FTC acknowledges that identity theft victims must spend countless hours and large amounts of money repairing the impact to their good name and credit record.[7] Identity thieves use stolen PII such as Social Security numbers for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.[8]

19. Once PII is stolen, particularly Social Security numbers, fraudulent use of that information and damage to victims may continue for years.

20. Social Security numbers, for example, are among the worst kind of personal information to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change.

21. The Social Security Administration has warned that identity thieves can use an individual's Social Security number to apply for additional credit lines. Such fraud may go undetected until debt collection calls commence months, or even years, later.[9] This time lag between when harm occurs versus when it is discovered, and also

---

6 *Id.*

7 *Guide for Assisting Identity Theft Victims*, FTC (Sep. 2013), *available at*: https://www.consumer.ftc.gov/articles/pdf-0119-guide-assisting-id-theft-victims.pdf (the "FTC Guide").

8 *Id.*

9 *Identity Theft and Your Social Security Number*, Social Security Administrative *available at* http://www.ssa.gov/pubs/EN-05-10064.pdf.

between when PII is stolen and when it is used, compounds an identity theft victim's ability to detect and address the harm.

22. According to the GOA, which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[10]

23. Stolen Social Security numbers also make it possible for thieves to file fraudulent tax returns, file for unemployment benefits, or apply for a job using a false identity. Each of these fraudulent activities is difficult to detect. An individual may not know that his or her Social Security number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

24. This data, as one would expect, demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information, personally identifiable information and Social Security numbers are worth more than 10x on the black market."[11]

---

[10] *Report to Congressional Requesters*, GAO, at 29 (June 2007), *available at* http://www.gao.gov/new.items/d07737.pdf.

[11] Time Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, (Feb. 6, 2015), *available at* http://www.itworld.com/article/2880960/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html.

25. What is more, it is no easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security Number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

26. Even then, a new Social Security number may not be effective. According to Julie Ferguson of the Identity Theft Resource Center, "The credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[12]

27. With access to a person's PII, criminals are capable of conducting myriad nefarious actions in addition to emptying a victim's bank account. Identity thieves also commit various types of government fraud, such as: obtaining a driver's license or official identification card in the victim's name with the thief's picture; using the victim's name and Social Security number to steal government benefits; and filing a fraudulent tax return using the victim's information. Worse, identity thieves may obtain a job using a victim's Social Security number, rent a house, receive medical services in the victim's name, or give the victim's information to police during an arrest, resulting in an arrest warrant being issued in the victim's name.[13]

---

[12] Bryan Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), *available at* http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft (last visited August 31, 2018).

[13] FTC Guide, *supra* n.9.

28. PII is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black-market" for a number of years.[14] As a result of large-scale data breaches, identity thieves and cyber criminals have openly posted stolen credit card numbers, Social Security numbers, healthcare information, and other PII directly on various Internet websites making the information publicly available. These networks and markets consist of hundreds of thousands, if not millions, of nefarious actors who view and access the PII.

29. In one study from 2010, researchers found hundreds of websites displaying stolen PII. Strikingly, none of these websites were blocked by Google's safeguard filtering mechanism—the "Safe Browsing list." The study concluded:

> It is clear from the current state of the credit card black-market that cyber criminals can operate much too easily on the Internet. They are not afraid to put out their email addresses, in some cases phone numbers and other credentials in their advertisements. It seems that the black market for cyber criminals is not underground at all. In fact, it's very "in your face."[15]

30. In another report about health-care related identity theft fraud sponsored by Experian indicated that the "average total cost to resolve an identity theft-related incident…came to about $20,000." Further, a majority of the victims were forced to pay out-of-pocket costs for health care they did not receive in order to restore coverage. Moreover, almost 50 percent of the victims lost their health care coverage as a result

[14] FTC Guide, *supra* n.9.
[15] *The "Underground" Credit Card Blackmarket*, StopTheHacker, *available at:* http://credit-help.pro/credit/59241

of the incident, while nearly one-third said their insurance premiums went up after the event. Forty percent of the customers were never able to resolve their identity theft at all. Indeed, data breaches and identity theft have a crippling effect on individuals and detrimentally impact the entire economy as a whole.[16]

B. Defendant Obtains, Collects, and Stores Plaintiffs' and Class Members' PII

31. Defendant FOI is one of the largest conglomerates of orthopaedic offices based in Tampa Bay, Florida.

32. As one of the largest orthopaedic conglomerates, FOI collects, stores, and maintains a massive amount of protected health information and other personally identifiable data on its customers and/or patients.

33. As a condition of providing health care services, Defendant requires that its patients entrust it with certain personal information. In its ordinary course of business, Defendant maintains personal information, including the name, address, zip code, date of birth, Social Security number, personal medical information, and protected health information of each current and former patient.

34. By obtaining, collecting, using, and deriving benefits from Plaintiffs' and the Class Members' PII, Defendant assumed legal and equitable duties to those individuals. Defendant knew or should have known that it were responsible for protecting Plaintiffs' and Class Members' PII from disclosure.

35. Plaintiffs and the Class Members, as current and former patients, relied

[16] Elinor Mills, *Study: Medical identity theft is costly for victims*, CNET (March 3, 2010) https://www.cnet.com/news/study-medical-identity-theft-is-costly-for-victims/

on Defendant to keep their PII confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

C. Defendant's Privacy Policy and Agreements to Keep PII Confidential

36. FOI represented to Plaintiffs and Class Members that it would protect their PII.

37. Through its Privacy Policy, FOI provides patients with policies concerning those patients' confidentiality and privacy rights.

38. Defendant created these policies, representations, and requirements, and publicly advertised them on its website as a means of increasing the value of its relationships with patients, thus allowing it to charge consumers higher rates under the guise of enhanced security and information security practices. These agreements were the same for all of Defendant's patients, including Plaintiffs and Class Members.

D. The Data Disclosure

39. On or about April 9, 2020, Defendant's computer system suffered a ransomware attack that encrypted the data stored on its servers. FOI acknowledged that personal information of its patients was exposed during the incident containing personal and protected information, including Plaintiffs' and Class Members' PII.[17]

[17] Notification Letter, Ex. A.

40. In addition to failing to secure Plaintiffs' and Class Members' PII, Defendant also failed to adequately investigate the breach to determine the scope and expanse of the breach and failed to notify its patients within a reasonable time.

41. On or about June 18, 2020—*more than two months after the breach*—FOI finally publicly revealed the Data Disclosure to current and former patients.

42. Upon information and belief, the June 18, 2020, letter was the first notice received by FOI's current and former patients that their PII had been wrongly disclosed.

43. The June 18, 2020, letter failed to advise of the actual date of the Data Disclosure or why Defendant FOI waited more than two (2) months after discovering the incident to notify patients of the Data Disclosure.

44. Defendant prepared and drafted the Notification Letter. In deliberate disregard to the fact that the stolen sensitive, unprotected information was readily viewable by unauthorized third parties, Defendant downplayed the seriousness of the incident by informing Plaintiffs and the Class Members that "while we are not aware of the misuse of any information impacted by this incident, we are sending this letter to notify you about the incident and provide information about steps you *can* take to help protect your information" and further downplayed the seriousness by stating "We immediately began an internal invsestigation to secure our environment and restore impacted data."[18]

[18] Notification Letter, Ex. A.

45. These representations are just simple boilerplate language pulled off a common template, clearly evidencing Defendant's lack of concern for the seriousness of the Data Disclosure—wherein hackers gained access to Defendant's systems, encrypted that data, and, according to Defendant, likely exfiltrated that data.

46. Plaintiffs received their letters on or about June 27, 2020 nearly 3 months after the security incident was discovered. Due to the potential for further compromise, an exemplar of the letter is attached to this Complaint, as Exhibit A.

47. Defendant, however, failed to notify its patients, until approximately 70 days after the Data Disclosure. And yet, in its Notification Letter, Defendant makes reference to having engaged a third-party forensic investigator but did not provide any details concerning the efforts to investigate, did not notify if any law enforcement agencies were involved, or any other efforts to investigate and neutralize the theft and continued misuse of Defendant's patients' PII.

48. Continuing to downplay the very serious ramifications of the Data Disclosure, Defendant offered its patients an identity monitoring service, but you only have three months (i.e., September 30, 2020) to sign up for it, even though the security of that PII is forever compromised and Plaintiffs and Class Members are forever at risk of future misuse.

49. Defendant took no action to promptly notify its patients that were affected by the Data Disclosure.

50. Defendant, knowing that PII is subject to the strict privacy and security protections of HIPAA, and other standards and regulations, delayed and otherwise

failed to properly and timely provide notice to Plaintiffs and Class Members regarding the stolen PII.

51. Defendant has acknowledged the sensitive and confidential nature of the PII. To be sure, collection, maintaining, and protecting PII is vital to many of Defendant's business purposes. Defendant has acknowledged through conduct and statements that the misuse or inadvertent disclosure of PII can pose major privacy and financial risks to impacted individuals, and that under state law they may not disclose and must take reasonable steps to protect PII from improper release or disclosure. Despite the prevalence of public announcements of data breach and data security compromises, and despite its own acknowledgments of data breach and data security compromises, and despite its own acknowledgment of its duties to keep PII private and secure, Defendant failed to take appropriate steps to protect the PII of Plaintiffs and Class Members from being compromised.

52. The ramifications of Defendant's failure to keep its customers/patients' protected health information and other PII secure are long lasting and severe.

53. Based on the foregoing, the information compromised in the Data Disclosure is significantly more valuable than data breaches involving non-health information. The information compromised in the FOI Data Disclosure is impossible to "close" and difficult, if not impossible, to change—Social Security number, name, date of birth, address, medical information, and other PII.

54. Defendant designed and implemented its policies and procedures regarding the security of protected health information and PII.

55. Further, Defendant failed to notify Plaintiffs and Class Members whose protected health information and other PII was, or was reasonably believed to have been, accessed by unauthorized persons through the Data Disclosure in any manner, including but not limited to, written, telephone, electronic, or authorized substitute notice until more than two months afterward and notification letters were sent out shortly thereafter.

56. Upon information and belief, Defendant failed to effectively supervise Defendant's workforce (including both employees and independent contractors) on the policies and procedures with respect to the appropriate maintenance, use, and disclosure of protected health information and other PII.

57. Defendant's collective failure to protect and otherwise safeguard Defendant's computers resulted in the exposure of the protected health information and other PII of at least 100,000 patients and potentially in excess of 150,000 current and former patients.

58. Plaintiffs provided Defendant with their accurate protected health information and other PII. The stolen information contained unprotected PII. Class Members similarly provided Defendant with their accurate protected health information and other PII.

59. As a result of the delayed response and notification, Plaintiffs and Class Members had no idea their PII had been compromised, and that they were, and continued to be, at significant risk to identity theft and various other forms of personal, social, and financial harm.

60. The Data Disclosure not only reveals that Defendant failed to exercise reasonable care in storing and protecting Plaintiffs' and Class Members' PII; it exposed the PII of at least 100,000, and potentially in excess of 150,000 patients to fraud and misuse by unauthorized third parties. The affected individuals face a real, concrete, and actual risk of harm and future identity theft as the PII contained confidential biographical information.

61. As a consequence of the Data Disclosure, Plaintiffs and Class Members have suffered damages by taking measures to both deter and detect identity theft. Plaintiffs and Class Members have been required to take their valuable time and energy, which they otherwise would have dedicated to other life demands (such as work), and efforts to mitigate the actual and potential impact of the Data Disclosure on their lives including, *inter alia*; placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, closely reviewing and monitoring their credit reports and accounts for unauthorized activity, and filing police reports. This time has been lost forever and cannot be recaptured. In all manners of life in this country, time has constantly been recognized as compensable: indeed, for many consumers it is the way they are compensated; and even if retired from the workforce, consumers should be free of having to deal with the consequences of companies' wrongful conduct, as is the case here.

62. Without question, the PII of Plaintiffs and Class Members, particularly their Social Security numbers, protected health information, and dates of birth, can be

used for purposes of identity theft, and unfortunately, FOI's current and former patients are now, and for the rest of their lives will be, at a heightened risk of further identity theft and fraud.

E. Defendant's Data Disclosure Exposed Plaintiffs to Identity Theft and Monetary Injuries

63. Plaintiffs and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their PII.

64. Despite all of the publicly available knowledge of the continued compromises of PII, Defendant's approach to maintaining the privacy of Defendant's customers/patients' protected health information and other PII was lackadaisical, cavalier, reckless, or in the very least, negligent.

65. In all manners of life in this country, time has constantly been recognized as compensable, for many people it is the way they are compensated. Plaintiffs and Class Members should be free of having to deal with the consequences of Defendant's slippage.

66. The PII (including Social Security number) of Plaintiff Whitman's minor child, age 6, was provided only to two entities: 1) the hospital where she was born; and 2) Defendant. Plaintiff Whitman, on behalf of his minor child, has not received any data breach notifications from that hospital, but did receive a data breach notification from Defendant.

67. Shortly after the Data Disclosure occurred, Plaintiff Whitman's minor child's PII was used to file a fraudulent tax return in her name, which has required Plaintiff Whitman to incur substantial time and monetary damages attempting to resolve the repercussions of Defendant's security failures permitting the Data Disclosure to occur. Further, Plaintiff Whitman, on behalf of his minor child, contacted Kroll (Defendant's fraud resolution specialist), but received no help, forcing Plaintiff Whitman to engage professional assistance to resolve the fraud his minor child has experienced.

F. Defendant's Offered Credit Monitoring is Inadequate

68. Defendant offered Plaintiffs and Class Members a limited period of time of identity monitoring services from Kroll.

69. Defendant's offer is a woefully insufficient remedy for Defendant's Data Disclosure. As discussed above, victims of data breaches and other unauthorized disclosures commonly face multiple years of ongoing identity theft.

70. In addition, Defendant's offer does not address any compensation for the unauthorized release and disclosure of Plaintiffs' and Class Members' PII, including medical information.

71. Furthermore, Defendant's identity monitoring offer to Plaintiffs and Class Members squarely places the burden on Plaintiffs and Class Members, rather than Defendant, to investigate and protect themselves from Defendant's tortious acts resulting in the Data Disclosure. Defendant sent instructions "offering" the services to affected patients/customers recommending they sign up for the services.

72. Defendant has failed to provide appropriate and adequate compensation to Plaintiffs and Class Members victimized in this Data Disclosure.

73. It is incorrect to assume that reimbursing a consumer for financial loss due to fraud makes that individual whole again. On the contrary, after conducting a study, the U.S. Department of Justice's Bureau of Justice Statistics found that "among victims who had personal information used for fraudulent purposes, 29% spent a month or more resolving problems" and that "resolving the problems caused by identity theft [could] take more than a year for some victims."[19]

74. As a result of Defendant's failure to prevent the Data Disclosure, Plaintiffs and Class Members have suffered and will continue to suffer damages, including monetary losses, lost time, anxiety, and emotional distress. They have suffered or are at increased risk of suffering:

a. Actual identity theft;

b. Unauthorized use and misuse of their PII;

c. The loss of the opportunity to control how their PII is used;

d. The diminution in value of their PII;

e. The compromise, publication, and/or theft of their PII;

f. Out-of-pocket costs associated with the prevention, detection, recovery and remediation from identity theft or fraud;

g. Lost opportunity costs and lost wages associated with effort expended

[19] *Victims of Identity Theft*, 2012 (Dec. 2013) at 10, 11, *available at* https://www.bjs.gov/content/pub/pdf/vit12.pdf (last visited August 31, 2018).

and the loss of productivity from addressing and attempting to mitigate the actual and future consequences of the Data Disclosure, including but not limited to efforts spent researching how to prevent, detect, contest and recover from identity theft and fraud;

h. Costs associated with placing freezes on credit reports;

i. Delay in receipt of tax refund monies;

j. The diminished value of Defendant's goods and services they received;

k. Lost opportunity and benefits of electronically filing of income tax returns;

l. The imminent and certain impending injury flowing from potential fraud and identity theft posed by their PII being placed in the hands of criminals;

m. The continued risk to their PII, which remains in the possession of Defendant and is subject to further breaches so long as Defendant fails to undertake appropriate measures to protect the PII in its possession; and

n. Current and future costs in terms of time, effort and money that will be expended to prevent, detect, contest, remediate and repair the impact of the Data Disclosure for the remainder of the lives of Plaintiffs and Class Members.

G. Defendant's Conduct Violates HIPAA and Industry Standard Practices

75. Title II of HIPAA contains what are known as the Administrative Simplification provisions. 42 U.S.C. §§ 1301, *et seq*. These provisions require, among

other things, that the Department of Health and Human Services ("HHS") create rules to streamline the standards for handling PII like the data Defendant left unguarded. The HHS has subsequently promulgated five rules under authority of the Administrative Simplification provisions of HIPAA.

76. Defendant's Data Disclosure resulted from a combination of insufficiencies that indicate Defendant failed to comply with safeguards mandated by HIPAA regulations and industry standards. First, it can be inferred from Defendant's Data Disclosure that Defendant either failed to implement, or inadequately implemented, information security policies or procedures in place to protect Plaintiffs' and Class Members' PII.

77. In addition, Defendant's Data Disclosure could have been prevented if Defendant implemented HIPAA mandated, industry standard policies and procedures for securely disposing of PII when it was no longer necessary and/or had honored its obligations to its patients.

78. Defendant's security failures also include, but are not limited to:

a. Failing to maintain an adequate data security system to prevent data loss;

b. Failing to mitigate the risks of a data breach and loss of data;

c. Failing to ensure the confidentiality and integrity of electronic protected health information Defendant create, receive, maintain, and transmit in violation of 45 CFR 164.306(a)(1);

d. Failing to implement technical policies and procedures for electronic information systems that maintain electronic protected health

information to allow access only to those persons or software programs that have been granted access rights in violation of 45 CFR 164.312(a)(1);

e. Failing to implement policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 CFR 164.308(a)(1);

f. Failing to identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity in violation of 45 CFR 164.308(a)(6)(ii);

g. Failing to protect against any reasonably-anticipated threats or hazards to the security or integrity of electronic protected health information in violation of 45 CFR 164.306(a)(2);

h. Failing to protect against any reasonably-anticipated uses or disclosures of electronic protected health information that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 CFR 164.306(a)(3);

i. Failing to ensure compliance with HIPAA security standard rules by Defendant's workforce in violation of 45 CFR 164.306(a)(94);

j. Impermissibly and improperly using and disclosing protected health information that is and remains accessible to unauthorized persons in violation of 45 CFR 164.502, *et seq.*

79. Because Defendant has failed to comply with industry standards, while monetary relief may cure some of Plaintiffs' and Class Members' injuries, injunctive

relief is necessary to ensure Defendant's approach to information security is adequate and appropriate. Defendant still maintains the protected health information and other PII of Plaintiffs and Class Members; and without the supervision of the Court via injunctive relief, Plaintiffs' and Class Members' protected health information and other PII remains at risk of subsequent data disclosures.

CLASS ACTION ALLEGATIONS

80. Plaintiffs bring this suit as a class action on behalf of themselves and on behalf of all others similarly situated pursuant to Rule 1.220(b)(2) and (b)(3)) of the Florida Rules of Civil Procedure.

81. The Class that Plaintiffs seek to represent is defined as follows:

> All individuals in the United States who are current or former patients or customers of Defendant, whose PII was exposed and accessed, and who suffered injury or harm resulting from the dissemination of their PII.

82. Excluded from the Class are the officers, directors, and legal representatives of Defendant, and the judges and court personnel in this case and any members of their immediate families.

83. Numerosity. Florida Rule of Civil Procedure 1.220(a)(1). The Class Members are so numerous that joinder of all Members is impractical. While the exact number of Class Members is unknown to Plaintiffs at this time, based on information and belief, it is estimated to be at or above 100,000. The exact number is generally ascertainable by appropriate discovery as Defendant has knowledge of the customers/patients whose PII was disclosed by way of, at the very least, the list of

individuals to whom Defendant sent the Notification Letters.

84. Commonality. Florida Rule of Civil Procedure 1.220(a)(2) and (b)(3). There are questions of law and fact common to the Class, which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

a. Whether and to what extent Defendant had a duty to protect the PII of Class Members;

b. Whether Defendant was negligent in collecting and storing Plaintiffs' and Class Members' PII;

c. Whether Defendant had duties not to disclose the PII of Class Members to unauthorized third parties;

d. Whether Defendant took reasonable steps and measures to safeguard Plaintiffs' and Class Members' PII;

e. Whether Defendant failed to adequately safeguard the PII of Class Members;

f. Whether Defendant breached its duties to exercise reasonable care in handling Plaintiffs' and Class Members' PII by storing that information on computers and hard drives in the manner alleged herein, including failing to comply with industry standards;

g. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Disclosure;

h. Whether implied or express contracts existed between Defendant, on the one hand, and Plaintiffs and Class Members on the other;

i. Whether Defendant had respective duties not to use the PII of Class Members for non-business purposes;

j. Whether Defendant adequately, promptly, and accurately informed Plaintiffs and Class Members that their PII had been compromised;

k. Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard the PII of Class Members;

l. Whether Plaintiffs and Class Members are entitled to actual, damages, statutory damages, and/or punitive damages as a result of Defendant's wrongful conduct;

o. Whether Plaintiffs and Class Members are entitled to restitution as a result of Defendant's wrongful conduct;

p. Whether Plaintiffs and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Disclosure; and

q. Whether Plaintiffs and Class Members are entitled to identity theft protection for their respective lifetimes.

85. Typicality. Florida Rule of Civil Procedure 1.220(a)(3). Plaintiffs' claims are typical of those of other Class Members because Plaintiffs' PII, like that of every other Class Member, was disclosed by Defendant. Plaintiffs' claims are typical of those of the other Class Members because, *inter alia*, all Members of the Class were injured

through the common misconduct of Defendant. Plaintiffs are advancing the same claims and legal theories on behalf of themselves and all other Class Members, and there are no defenses that are unique to Plaintiffs. The claims of Plaintiffs and those of Class Members arise from the same operative facts and are based on the same legal theories.

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

87. Adequacy of Representation. Florida Rule of Civil Procedure 1.220(a)(4). Plaintiffs will fairly and adequately represent and protect the interests of the Class in that they have no disabling conflicts of interest that would be antagonistic to those of the other Members of the Class. Plaintiffs seeks no relief that is antagonistic or adverse to the Members of the Class and the infringement of the rights and the damages they have suffered are typical of other Class Members. Plaintiffs have retained counsel experienced in complex consumer class action litigation and in particular privacy class litigation, and Plaintiffs intend to prosecute this action vigorously.

88. Superiority of Class Action. Florida Rule of Civil Procedure 1.220(b)(3). The class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of class members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain class members, who could not individually afford to litigate a complex claim against large corporations, like Defendant. Further, even for those class members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

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

on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

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

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

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

93. Further, Defendant has acted or refused to act on grounds generally applicable to the Class and, accordingly, final injunctive or corresponding declaratory relief with regard to the Class Members as a whole is appropriate under the Florida Rules of Civil Procedure.

FIRST CAUSE OF ACTION
Negligence
(On Behalf of the Class)

94. Plaintiffs restate and reallege paragraphs 1 through 93 above as if fully set forth herein.

95. As a condition of their utilizing the services of Defendant, patients were obligated to provide Defendant with certain PII, including their date of birth, mailing

addresses, Social Security numbers, personal medical information, and protected health information.

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

97. Defendant has full knowledge of the sensitivity of the PII and the types of harm that Plaintiffs and Class Members could and would suffer if the PII were wrongfully disclosed.

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

99. Defendant had a duty to exercise reasonable care in safeguarding, securing, and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties. This duty includes, among other things, designing, maintaining, and testing Defendant's security protocols to ensure that Plaintiffs' and Class Members' information in Defendant's possession was adequately secured and protected, and that employees tasked with maintaining such information were adequately trained on security measures regarding the security of patients' personal and medical information.

100. Defendant also had a duty to have procedures in place to detect and

prevent the improper access and misuse of Plaintiffs' and Class Members' PII.

101. A breach of security, unauthorized access, and resulting injury to Plaintiffs and the Class Members was reasonably foreseeable, particularly in light of the growing amount of data breaches for health care providers and other industries.

102. Plaintiffs and Class Members were the foreseeable and probable victims of any inadequate security practices and procedures. Defendant knew or should have known of the inherent risks in collecting and storing the PII of Plaintiffs and the Class, the critical importance of providing adequate security of that PII, and that it had inadequate employee training and education and IT security protocols in place to secure the PII of Plaintiffs and the Class.

103. Defendant's own conduct created a foreseeable risk of harm to Plaintiffs and Class Members. Defendant's misconduct included, but was not limited to, its failure to take the steps and opportunities to prevent the Data Disclosure as set forth herein. Defendant's misconduct also included its decisions not to comply with industry standards for the safekeeping and unauthorized disclosure of the PII of Plaintiffs and Class Members.

104. Plaintiffs and the Class Members had no ability to protect their PII that was in Defendant's possession.

105. Defendant was in a position to protect against the harm suffered by Plaintiffs and Class Members as a result of the Data Disclosure.

106. Defendant had and continues to have a duty to adequately disclose that the PII of Plaintiffs and Class Members within Defendant's possession might have

been compromised, how it was compromised, and precisely the types of information that were compromised and when. Such notice was necessary to allow Plaintiffs and the Class Members to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their PII by third parties.

107. Defendant had a duty to employ proper procedures to prevent the unauthorized dissemination of the PII of Plaintiffs and Class Members.

108. Defendant has admitted that the PII of Plaintiffs and Class Members was wrongfully disclosed to unauthorized third persons as a result of the Data Disclosure.

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

110. Defendant improperly and inadequately safeguarded the PII of Plaintiffs and Class Members in deviation of standard industry rules, regulations, and practices at the time of the Data Disclosure.

111. Defendant failed to heed industry warnings and alerts to provide adequate safeguards to protect customers/patients' PII in the face of increased risk of theft.

112. Defendant, through its actions and/or omissions, unlawfully breached its duty to Plaintiffs and Class Members by failing to have appropriate procedures in place to detect and prevent dissemination of its customers/patients' PII.

113. Defendant, through its actions and/or omissions, unlawfully breached its duty to adequately and timely disclose to Plaintiffs and Class Members the existence and scope of the Data Disclosure.

114. But for Defendant's wrongful and negligent breach of duties owed to Plaintiffs and Class Members, the PII of Plaintiffs and Class Members would not have been compromised.

115. There is a close causal connection between Defendant's failure to implement security measures to protect the PII of current and former patients and the harm suffered or risk of imminent harm suffered by Plaintiffs and the Class. Plaintiffs' and Class Members' PII was stolen and accessed as the proximate result of Defendant's failure to exercise reasonable care in safeguarding such PII by adopting, implementing, and maintaining appropriate security measures.

116. As a direct and proximate result of Defendant's negligence, Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity how their PII is used; (iii) the compromise, publication, and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Disclosure, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the

continued risk to their PII, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII of customers/patients and former customers/patients in its continued possession; (viii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Disclosure for the remainder of the lives of Plaintiffs and Class Members; and (ix) the diminished value of Defendant's goods and services Plaintiffs and Class Members received.

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

SECOND CAUSE OF ACTION
Invasion of Privacy
(On Behalf of the Class)

118. Plaintiffs restate and reallege paragraphs 1 through 93 above as if fully set forth herein.

119. Plaintiffs and Class Members had a legitimate expectation of privacy to their PII and were entitled to the protection of this information against disclosure to unauthorized third parties.

120. Defendant owed a duty to its customers/patients, including Plaintiffs and Class Members, to keep their PII contained as a part thereof, confidential.

121. Defendant failed to protect and released to unknown and unauthorized

third parties the PII of Plaintiffs and Class Members.

122. Defendant allowed unauthorized and unknown third parties unfettered access to and examination of the PII of Plaintiffs and Class Members, by way of Defendant's failure to protect the PII from unauthorized disclosure.

123. The unauthorized release to, custody of, and examination by unauthorized third parties of the PII of Plaintiffs and Class Members, especially where the information includes Social Security numbers and dates of birth, is highly offensive to a reasonable person.

124. The intrusion was into a place or thing, which was private and is entitled to be private. Plaintiffs and Class Members disclosed their PII to Defendant as part of their use of Defendant's services, but privately with an intention that the PII would be kept confidential and would be protected from unauthorized disclosure. Plaintiffs and Class Members were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization.

125. The Data Disclosure at the hands of Defendant constitutes an intentional interference with Plaintiffs' 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.

126. As a proximate result of the above acts and omissions of Defendant, the PII of Plaintiffs and Class Members was disclosed to and used by third parties without authorization, causing Plaintiffs and Class Members to suffer damages.

127. Unless and until enjoined and restrained by order of this Court,

Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiffs and Class Members in that the PII maintained by Defendant can be viewed, distributed, and used by unauthorized persons. Plaintiffs 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 Plaintiffs and the Class.

THIRD CAUSE OF ACTION
Breach of Implied Contract
(On Behalf of the Class)

128. Plaintiffs restate and reallege paragraphs 1 through 93 above as if fully set forth herein.

129. Plaintiffs and Class Members were required to provide their PII, including names, addresses, Social Security numbers, dates of birth, medical condition(s) and other personal information, to Defendant as a condition of their use of Defendant's services.

130. Plaintiffs and Class Members paid money to Defendant in exchange for goods and services, as well as Defendant's promises to protect their protected health information and other PII from unauthorized disclosure.

131. In its written Privacy Policy, Defendant expressly promised Plaintiffs and Class Members that Defendant would only disclose protected health information and other PII under certain circumstances, none of which relate to the Data Disclosure.

132. Defendant promised to comply with HIPAA standards and to make sure that Plaintiffs' and Class Members' protected health information and other PII would remain protected.

133. Implicit in the agreement between the Defendant's patients, including Plaintiffs and Class Members, to provide protected health information and other PII, and Defendant's acceptance of such protected health information and other PII, was Defendant's obligation to use the PII of its patients for business purposes only, take reasonable steps to secure and safeguard that protected health information and other PII, and not make unauthorized disclosures of the protected health information and other PII to unauthorized third parties.

134. Further, implicit in the agreement, Defendant was obligated to provide Plaintiffs and Class Members with prompt and sufficient notice of any and all unauthorized access and/or theft of their protected health information and other PII.

135. Without such implied contracts, Plaintiffs and Class Members would not have provided their protected health information and other PII to Defendant.

136. Defendant had an implied duty to reasonably safeguard and protect the PII of Plaintiffs and Class Members from unauthorized disclosure or uses.

137. Additionally, Defendant implicitly promised to retain this PII only under conditions that kept such information secure and confidential.

138. Plaintiffs and Class Members fully performed their obligations under the implied contract with Defendant; however, Defendant did not.

139. Defendant breached the implied contracts with Plaintiffs and Class Members by failing to reasonably safeguard and protect Plaintiffs and Class Members' PII, which was compromised as a result of the Data Disclosure.

140. Defendant further breached the implied contracts with Plaintiffs and

Class Members by failing to comply with its promise to abide by HIPAA.

141. Defendant further breached the implied contracts with Plaintiffs and Class Members by failing to ensure the confidentiality and integrity of electronic protected health information Defendant created, received, maintained, and transmitted in violation of 45 CFR 164.306(a)(1).

142. Defendant further breached the implied contracts with Plaintiffs and Class Members by failing to implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights in violation of 45 CFR 164.312(a)(1).

143. Defendant further breached the implied contracts with Plaintiffs and Class Members by failing to implement policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 CFR 164.308(a)(1).

144. Defendant further breached the implied contracts with Plaintiffs and Class Members by failing to identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity in violation of 45 CFR 164.308(a)(6)(ii).

145. Defendant further breached the implied contracts with Plaintiffs and Class Members by failing to protect against any reasonably anticipated threats or hazards to the security or integrity of electronic protected health information in violation of 45 CFR 164.306(a)(2).

146. Defendant further breached the implied contracts with Plaintiffs and

Class Members by failing to protect against any reasonably anticipated uses or disclosures of electronic protected health information that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 CFR 164.306(a)(3).

147. Defendant further breached the implied contracts with Plaintiffs and Class Members by failing to ensure compliance with the HIPAA security standard rules by its workforce violations in violation of 45 CFR 164.306(a)(94).

148. Defendant further breached the implied contracts with Plaintiffs and Class Members by impermissibly and improperly using and disclosing protected health information that is and remains accessible to unauthorized persons in violation of 45 CFR 164.502, *et seq*.

149. Defendant further breached the implied contracts with Plaintiffs and Class Members by failing to design, implement, and enforce policies and procedures establishing physical administrative safeguards to reasonably safeguard protected health information, in compliance with 45 CFR 164.530(c).

150. Defendant further breached the implied contracts with Plaintiffs and Class Members by otherwise failing to safeguard Plaintiffs' and Class Members' PII.

151. Defendant's failures to meet these promises constitute breaches of the implied contracts.

152. Because Defendant allowed unauthorized access to Plaintiffs' and Class Members' PII and failed to safeguard the PII, Defendant breached its contracts with Plaintiffs and Class Members.

153. A meeting of the minds occurred, as Plaintiffs and Class Members agreed, *inter alia*, to provide accurate and complete PII and to pay Defendant in exchange for Defendant's agreement to, *inter alia*, protect their PII.

154. Defendant breached its contracts by not meeting the minimum level of protection of Plaintiffs' and Class Members' protected health information and other PII, because Defendant did not prevent against the breach of at least 100,000, and potentially exceeding 150,000, customer/patients' PII.

155. Furthermore, the failure to meet its confidentiality and privacy obligations resulted in Defendant providing goods and services to Plaintiffs and Class Members that were of a diminished value.

156. As a direct and proximate result of Defendant's breach of its implied contracts with Plaintiffs and Class Members, Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity how their PII is used; (iii) the compromise, publication, and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Disclosure, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their PII, which remain in Defendant's possession and is subject to further unauthorized

disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII of customers/patients and former customers/patients in its continued possession; (viii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Disclosure for the remainder of the lives of Plaintiffs and Class Members; and (ix) the diminished value of Defendant's goods and services they received.

157. As a direct and proximate result of Defendant's breach of its implied contracts with Plaintiffs and Class Members, Plaintiffs and Class Members have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

FOURTH CAUSE OF ACTION
Negligence Per Se
(On Behalf of the Class)

158. Plaintiffs restate and reallege paragraphs 1 through 93 above as if fully set forth herein.

159. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant's, of failing to use reasonable measures to protect PII. The FTC publications and orders described above also form part of the basis of Defendant's duty in this regard.

160. Defendant violated Section 5 of the FTC Act by failing to use reasonable

measures to protect PII and not complying with applicable industry standards described herein. Defendant's conduct was particularly unreasonable given the nature and amount of PII it obtained and stored, and the foreseeable consequences of a Data Disclosure for companies of Defendant's magnitude, including, specifically, the immense damages that would result to Plaintiffs and Class Members.

161. Defendant's violations of Section 5 of the FTC Act constitute negligence *per se*.

162. Plaintiffs and Class Members are within the class of persons that the FTC Act was intended to protect.

163. The harm that occurred as a result of the Data Disclosure is the type of harm the FTC Act was 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 and deceptive practices, caused the same harm as that suffered by Plaintiffs and the Class Members.

164. As a direct and proximate result of Defendant's negligence *per se*, Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity how their PII is used; (iii) the compromise, publication, and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Disclosure, including but not limited to efforts

spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their PII, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII of customers/patients and former customers/patients in its continued possession; (viii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Disclosure for the remainder of the lives of Plaintiffs and Class Members; and (ix) the diminished value of Defendant's goods and services they received.

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

FIFTH CAUSE OF ACTION
Unjust Enrichment
(On Behalf of the Class)

166. Plaintiffs restate and reallege paragraphs 1 through 93 above as if fully set forth herein.

167. Plaintiffs and Class Members conferred a monetary benefit on Defendant. Specifically, they purchased goods and services from Defendant and provided Defendant with their PII. In exchange, Plaintiffs and Class Members should have received from Defendant the goods and services that were the subject of the

transaction and should have been entitled to have Defendant protect their PII with adequate data security.

168. Defendant knew that Plaintiffs and Class Members conferred a benefit on Defendant and accepted and have accepted or retained that benefit. Defendant profited from the purchases and used the PII of Plaintiffs and Class Members for business purposes.

169. The amounts Plaintiffs and Class Members paid for Defendant's goods and services were used, in part, to pay for the administrative costs of data management and security.

170. Under the principles of equity and good conscience, Defendant should not be permitted to retain the money belonging to Plaintiffs and Class Members, because Defendant failed to implement the data management and security measures that are mandated by industry standards.

171. Defendant failed to secure the PII of Plaintiffs and Class Members and, therefore, did not provide full compensation for the benefit Plaintiffs and Class Members provided.

172. Defendant acquired the PII through inequitable means in that Defendant failed to disclose the inadequate security practices previously alleged.

173. If Plaintiffs and Class Members knew that Defendant would not secure their PII using adequate security, they would not have made used the services of Defendant.

174. Plaintiffs and Class Members have no adequate remedy at law.

175. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity how their PII is used; (iii) the compromise, publication, and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Disclosure, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their PII, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII of customers/patients and former customers/patients in its continued possession; (viii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Disclosure for the remainder of the lives of Plaintiffs and Class Members; and (ix) the diminished value of Defendant's goods and services they received.

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

177. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiffs and Class Members, proceeds that Defendant unjustly received from them. In the alternative, Defendant should be compelled to refund the amounts that Plaintiffs and Class Members overpaid for Defendant's goods and services.

SIXTH CAUSE OF ACTION
Breach of Fiduciary Duty
(On Behalf of the Class)

178. Plaintiffs restate and reallege paragraphs 1 through 93 above as if fully set forth herein.

179. In light of the special relationship between Defendant and its customers/patients, whereby Defendant became a guardian of Plaintiffs' and Class Members' highly sensitive, confidential, personal, financial information, and other PII, Defendant was a fiduciary, created by its undertaking and guardianship of the PII, to act primarily for the benefit of its customers/patients, including Plaintiffs and Class Members, for: 1) the safeguarding of Plaintiffs' and Class Members' PII; 2) timely notify Plaintiffs and Class Members of a data breach or disclosure; and 3) maintain complete and accurate records of what and where Defendant's customers/patients' information was and is stored.

180. Defendant had a fiduciary duty to act for the benefit of Plaintiffs and Class Members upon matters within the scope of its customers/patients' relationship, in particular to keep secure the PII of its customers/patients.

181. Defendant breached its fiduciary duties to Plaintiffs and Class Members

by failing to diligently investigate the Data Disclosure to determine the number of Members affected in a reasonable and practicable period of time.

182. Defendant breached its fiduciary duties to Plaintiffs and Class Members by failing to protect Plaintiffs' and Class Members' protected health information and other PII.

183. Defendant breached its fiduciary duties to Plaintiffs and Class Members by failing to timely notify and/or warn Plaintiffs and Class Members of the Data Disclosure.

184. Defendant breached its fiduciary duties to Plaintiffs and Class Members by failing to ensure the confidentiality and integrity of electronic protected health information Defendant created, received, maintained, and transmitted, in violation of 45 CFR 164.306(a)(1).

185. Defendant breached its fiduciary duties to Plaintiffs and Class Members by failing to implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights in violation of 45 CFR 164.312(a)(1).

186. Defendant breached its fiduciary duties to Plaintiffs and Class Members by failing to implement policies and procedures to prevent, detect, contain, and correct security violations, in violation of 45 CFR 164.308(a)(1).

187. Defendant breached its fiduciary duties to Plaintiffs and Class Members by failing to identify and respond to suspected or known security incidents; mitigate,

to the extent practicable, harmful effects of security incidents that are known to the covered entity in violation of 45 CFR 164.308(a)(6)(ii).

188. Defendant breached its fiduciary duties to Plaintiffs and Class Members by failing to protect against any reasonably-anticipated threats or hazards to the security or integrity of electronic protected health information in violation of 45 CFR 164.306(a)(2).

189. Defendant breached its fiduciary duties to Plaintiffs and Class Members by failing to protect against any reasonably-anticipated uses or disclosures of electronic protected health information that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 CFR 164.306(a)(3).

190. Defendant breached its fiduciary duties to Plaintiffs and Class Members by failing to ensure compliance with the HIPAA security standard rules by its workforce in violation of 45 CFR 164.306(a)(94).

191. Defendant breached its fiduciary duties to Plaintiffs and Class Members by impermissibly and improperly using and disclosing protected health information that is and remains accessible to unauthorized persons in violation of 45 CFR 164.502, *et seq.*

192. Defendant breached its fiduciary duties to Plaintiffs and Class Members by otherwise failing to safeguard Plaintiffs' and Class Members' PII.

193. As a direct and proximate result of Defendant's breaches of its fiduciary duties, Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity how their PII is

used; (iii) the compromise, publication, and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Disclosure, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their PII, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII of customers/patients and former customers/patients in its continued possession; (viii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Disclosure for the remainder of the lives of Plaintiffs and Class members; and (ix) the diminished value of Defendant's goods and services they received.

194. As a direct and proximate result of Defendant's breaches of its fiduciary duties, Plaintiffs and Class Members have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

SEVENTH CAUSE OF ACTION
Violation of Florida's Deceptive and Unfair Trade Practices Act
(On Behalf of the Class)

195. Plaintiffs restate and reallege paragraphs 1 through 93 above as if fully set forth herein.

196. Plaintiffs and the Class Members are "consumers." Fla. Stat. § 501.203(7).

197. Plaintiffs and Class Members purchased "things of value" insofar as products and services from Defendant. These purchases were made primarily for personal, family, health-related, or household purposes. Fla. Stat. § 501.203(9).

198. Defendant engaged in the conduct alleged in this Complaint by advertising and entering into transactions intended to result, and which did result, in the sale, rental of goods, services, and/or property to consumers, including Plaintiffs and the Class Members. Fla. Stat. § 501.203(8).

199. Defendant engaged in, and its acts and omissions affected trade and commerce. Defendant's acts, practices, and omissions were done in the course of Defendant's business of advertising, marketing, offering to sell, and selling and/or renting goods and services throughout Florida and the United States. Fla. Stat. § 501.203(8).

200. Defendant, headquartered and operating in Florida, engaged in deceptive, unfair, and unlawful trade acts or practices in the conduct of trade or commerce, in violation of Fla. Stat. § 501.204(1), including but not limited to the following:

a. charging a premium for the goods and services, implicitly representing that the premium would be used to protect Plaintiffs' and Class Members' protected health information and other PII;

b. representing (through advertisements and other publication) that it maintained, but in fact failed to maintain adequate computer systems and data security practices to safeguard PII;

c. representing (through advertisements and other publication) that its data security practices were adequate, but in fact failed to disclose that its computer systems and data security practices were inadequate to safeguard PII from theft;

d. failure to timely and accurately disclose the Data Disclosure to Plaintiffs and the Class Members;

e. continued acceptance of credit and debit card payments and storage of other PII after Defendant knew or should have known of the Data Disclosure and before it allegedly remediated the Data Disclosure;

201. This conduct is considered unfair methods of competition, and constitute unfair and unconscionable acts and practices. Fla. Stat. § 501.204(1).

202. As a direct and proximate result of Defendant's violation of Florida's Deceptive and Unfair Trade Practices Act ("FDUTPA"), Plaintiffs and the Class Members suffered actual damages by paying a premium for Defendant's goods and services with the understanding that at least part of the premium would be applied toward sufficient and adequate information security practices that comply with

industry standards, when in fact no portion of that premium was applied toward sufficient and adequate information security practices. Fla. Stat. § 501.211(2).

203. Also as a direct result of Defendant's knowing violation of FDUTPA, Plaintiffs and Class Members are not only entitled to actual damages, but also declaratory judgment that Defendant's actions and practices alleged herein violate FDUTPA, and injunctive relief, including, but not limited to:

a. Ordering that Defendant engage third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

b. Ordering that Defendant engage third-party security auditors and internal personnel to run automated security monitoring;

c. Ordering that Defendant audit, test, and train its security personnel regarding any new or modified procedures;

d. Ordering that Defendant segment PII by, among other things, creating firewalls and access controls so that if one area of Defendant is compromised, hackers cannot gain access to other portions of Defendant's systems;

e. Ordering that Defendant purge, delete, and destroy in a reasonable secure manner PII not necessary for Defendant's provisions of services;

f. Ordering that Defendant conduct regular database scanning and securing checks;

g. Ordering that Defendant routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and

h. Ordering Defendant to meaningfully educate its customers about the threats they face as a result of the loss of their financial and personal information to third parties, as well as the steps Defendant's customers must take to protect themselves.

Fla. Stat. § 501.211(1).

204. Plaintiffs bring this action on behalf of themselves and the Class Members for the relief requested above and for the public benefit in order to promote the public interests in the provision of truthful, fair information to allow consumers to make informed purchasing decisions and to protect Plaintiffs and the Class Members and the public from Defendant's unfair methods of competition and unfair, deceptive, fraudulent, unconscionable, and unlawful practices. Defendant's wrongful conduct as alleged in this Complaint has had widespread impact on the public at large.

205. The above unfair and deceptive practices and acts by Defendant were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to Plaintiffs and the Class Members that they could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

206. Defendant knew or should have known that the lack of data security practices were inadequate to safeguard the Class Members' PII and that the risk of a data disclosure or theft was high.

207. Defendant's actions and inactions in engaging in the unfair practices and deceptive acts described herein were negligent, knowing and willful, and/or wanton and reckless.

208. Plaintiffs and the Class Members seek relief under Florida Deceptive and Unfair Trade Practices Act, Fla. Stat. §§ 501.201, *et seq.*, including, but not limited to, damages, injunctive relief, and attorneys' fees and costs, and any other just and proper relief.

EIGHTH CAUSE OF ACTION
Breach of Confidence
(On Behalf of the Class)

209. Plaintiffs restate and reallege paragraphs 1 through 93 above as if fully set forth herein.

210. At all times during Plaintiffs' and Class Members' interactions with Defendant, Defendant was fully aware of the confidential and sensitive nature of Plaintiffs' and Class Members' protected health information and other PII that Plaintiffs and Class Members provided to Defendant.

211. As alleged herein and above, Defendant's relationship with Plaintiffs and Class Members was governed by terms and expectations that Plaintiffs' and Class Members' protected health information and other PII would be collected, stored, and protected in confidence, and would not be disclosed to unauthorized third parties.

212. Plaintiffs and Class Members provided their respective protected health information and PII to Defendant with the explicit and implicit understandings that Defendant would protect and not permit the protected health information and other PII to be disseminated to any unauthorized parties.

213. Plaintiffs and Class Members also provided their respective protected health information and PII to Defendant with the explicit and implicit understandings that Defendant would take precautions to protect that protected health information and other PII from unauthorized disclosure.

214. Defendant voluntarily received in confidence Plaintiffs' and Class Members' protected health information and other PII with the understanding that protected health information and other PII would not be disclosed or disseminated to the public or any unauthorized third parties.

215. Due to Defendant's failure to prevent, detect, and avoid the Data Disclosure from occurring by, *inter alia*, following best information security practices to secure Plaintiffs' and Class Members' protected health information and other PII, Plaintiffs' and Class Members' protected health information and PII was disclosed and misappropriated to unauthorized third parties beyond Plaintiffs' and Class Members' confidence, and without their express permission.

216. As a direct and proximate cause of Defendant's actions and/or omissions, Plaintiffs and Class Members have suffered damages.

217. But for Defendant's disclosure of Plaintiffs' and Class Members' protected health information and other PII in violation of the parties' understanding

of confidence, their protected health information and other PII would not have been compromised, stolen, viewed, accessed, and used by unauthorized third parties. Defendant's Data Disclosure was the direct and legal cause of the theft of Plaintiffs' and Class Members' protected health information and other PII, as well as the resulting damages.

218. The injury and harm Plaintiffs and Class Members suffered was the reasonably foreseeable result of Defendant's unauthorized disclosure of Plaintiffs' and Class Members' protected health information and other PII. Defendant knew or should have known its computer systems and technologies for accepting and securing Plaintiffs' and Class Members' protected health information and other PII had numerous security vulnerabilities.

219. As a direct and proximate result of Defendant's breaches of confidence, Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity how their PII is used; (iii) the compromise, publication, and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Disclosure, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their PII, which remain in Defendant's possession and is subject to

further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII of customers/patients and former patients in its continued possession; (viii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Disclosure for the remainder of the lives of Plaintiffs and Class Members; and (ix) the diminished value of Defendant's goods and services they received.

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

PRAYER FOR RELIEF

WHEREFORE Plaintiffs on behalf of themselves and all others similarly situated, pray for relief as follows:

a. For an Order certifying the Class as defined herein, and appointing Plaintiffs and thier Counsel to represent the Class;

b. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiffs' and the Class Members' PII, and from refusing to issue prompt, complete, and accurate disclosures to Plaintiffs and Class Members;

c. For equitable relief compelling Defendant to use appropriate cyber security

methods and policies with respect to PII collection, storage, and protection, and to disclose with specificity to Class Members the type of PII compromised;

d. For an award of damages, including actual, nominal, and consequential damages, as allowed by law in an amount to be determined;

e. For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;

f. For prejudgment interest on all amounts awarded; and

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

DEMAND FOR JURY TRIAL

Plaintiffs hereby demand a trial by jury on all issues so triable.

Dated: October 8, 2021

Respectfully submitted,

/s/ John A. Yanchunis

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

WILLIAM 'BILLY' PEERCE HOWARD
Billy@TheConsumerProtectionFirm.com
AMANDA J. ALLEN
Amanda@TheConsumerProtectionFirm.com
THE CONSUMER PROTECTION FIRM
4030 Henderson Boulevard

Tampa, FL 33629
(813) 500-1500 Telephone
(813) 435-2369 Facsimile

Attorneys for Plaintiffs and the Proposed Class