

FILED

UNITED STATES DISTRICT COURT
FOR THE MIDDLE DISTRICT OF FLORIDA

2016 MAR 18 AM 8:46

STUART KAPLAN, Individually, and on
Behalf of All Others Similarly Situated,

Plaintiff,

v.

21ST CENTURY ONCOLOGY
HOLDINGS, INC.

Defendant.

Civil Action No. _____

JURY TRIAL DEMANDED

2:16-CV-210-FTM-38CM

CLASS ACTION COMPLAINT

Plaintiff Stuart Kaplan ("Plaintiff"), makes the following allegations based on his personal knowledge, information and belief and the investigation of his counsel concerning the exposure to a third party of his personal information and that of the Class (as defined below), including medical records, as a result of an unauthorized third party illegally obtaining patient information provided to and maintained in a database by Defendant 21st Century Oncology Holdings, Inc. (the "Data Breach"). The Data Breach has resulted and will result in financial and other injury and damage to Plaintiff and the members of the Class.

FACTUAL ALLEGATIONS

I. On March 4, 2016, 21st Century Oncology Holdings, Inc. ("21st Century" or the "Company") announced that it was advised on November 13, 2015, by the Federal

Bureau of Investigation (the “FBI”) of the Data Breach. According to the Company’s 8-K filed with the SEC on March 4, 2016, the Company “determined that the intruder may have accessed the database on October 3, 2015, which contained the personal information of some patients (including patient name, social security number, physician’s name, diagnoses and treatment and insurance information).” The 8-K acknowledged that the information of approximately 2.2 million current and former patients of the Company (the “Affected Individuals”) may have been copied and transferred as a result of the Data Breach.

2. Despite the fact that it was storing sensitive personal information that it knew was valuable to, and vulnerable to a cyber-attack, 21st Century failed to take the necessary security precautions that could have protected the Affected Individuals’ data. Instead, 21st Century used inadequate data security practices that exposed the Affected Individuals’ personal data to hackers.

3. The 21st Century database (“Database”) included the types of information that federal and state law requires companies to take security measures, and indeed extra security measures, to protect: names, Social Security numbers, health care ID numbers and insurance information, and perhaps most sensitive, confidential medical records, such as physician names, diagnoses and treatment (“Personal Information”).

4. Defendant made repeated promises and representations to the Affected Individuals, in person, by mail or on their website, that they were protecting this sensitive Personal Information and would provide reasonable security in accordance with federal and state law. However, those promises and representations were not fulfilled. If 21st

Century had taken the required security steps, the Affected Individuals' sensitive Personal Information would not have been accessible by unauthorized third parties.

5. As a result of the 21st Century Data Breach, Affected Individuals have been harmed or exposed to harm, which threat may continue indefinitely. Now that their sensitive Personal Information has been exposed, Affected Individuals must worry about being victimized throughout the rest of their lives and spend countless hours to combat identity theft.

JURISDICTION AND VENUE

6. This Court has subject matter jurisdiction over this action under 28 U.S.C. § 1332(d)(2) because this is a class action wherein the amount in controversy exceeds the sum or value of \$5,000,000, exclusive of interest and costs, there are more than 100 members in each of the proposed classes, and at least one member of the Class is a citizen of a state different from Defendant.

7. This Court has personal jurisdiction over Defendant because Defendant's principal place of business is in the state of Florida, in this District.

8. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(b) because a substantial part of the events or omissions giving rise to the claims occurred in, was directed to, and/or emanated from this District.

PARTIES

9. At all relevant times, Plaintiff Stuart Kaplan resided and continues to reside in the State of Florida. 21st Century collected and received Plaintiff Kaplan's Personal Information and maintained it in its database. Plaintiff Kaplan received a letter from 21st

Century informing him that his Personal Information may have been compromised as a result of the 21st Century Data Breach. Plaintiff Kaplan now must engage in stringent monitoring of, among other things, his financial accounts, tax filings, and health insurance claims. As a result of the 21st Century Data Breach, Mr. Kaplan has spent hours addressing issues arising from the 21st Century Data Breach.

10. Defendant 21st Century is a Delaware corporation with its principal executive offices located at 2270 Colonial Boulevard, Fort Myers, Florida. 21st Century is the largest global, physician led provider of integrated cancer care services. As of December 31, 2015, the Company operated 181 treatment centers, including 145 centers in the U.S. across 17 states.

ADDITIONAL FACTUAL ALLEGATIONS

11. As a health care provider, 21st Century collects, receives, and accesses their patients' extensive individually identifiable Personal Information, including health record information. These records include information such as individually-identifiable health information pertaining to the individual patient's medical history, diagnosis codes, payment and billing records, test records, dates of service, and such health and treatment information necessary to process health insurance claims.

I. Defendant's Promise to Protect Personal Information

12. Defendant made promises to the Affected Individuals that it would protect their Personal Information, including in privacy notices provided to the Affected Individuals, as required by federal and state laws and regulations, including HIPAA.

13. On information and belief, 21st Century's website made similar promises regarding its privacy and security policies. The privacy policy on the website for 21st Century apparently has now been disabled or removed.

II. Defendant Had an Obligation to Protect Personal Information under Federal and State Law and Applicable Standards of Care

14. Defendant is covered by HIPAA (see 54 C.F.R. § 160.102) and as such is required to comply with the HIPAA Privacy Rule and Security Rule, 45 CFR Part 160 and Part 164, Subparts A and E ("Standards for Privacy of Individually Identifiable Health Information").

15. HIPAA limits the permissible uses of "protected health information" and prohibits unauthorized disclosures of "protected health information." Personally identifiable health information of patients, including names and social security numbers, is protected under HIPAA, even if no specific diagnostic or treatment information is disclosed.

16. HIPAA requires that Defendant implement appropriate safeguards for this type of Personal Information.¹ HIPPA also requires that, among other things, Defendant:

- a) 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, see 45 CFR § 164.312(a)(1);

¹ 45 C.F.R. § 164.530(c)(1) (2009).

- b) Implement policies and procedures to prevent, detect, contain, and correct security violations, *See* 45 CFR § 164.306(a)(1);
- c) Protect against any reasonably anticipated threats or hazards to the security or integrity of electronic protected health information, *See* 45 CFR § 164.306(a)(2); and
- d) Protect against reasonably anticipated uses or disclosures of electronic protected health information that are not permitted under the privacy rules regarding individually identifiable health information, *See* 45 CFR § 164.306(a)(3).

17. Gramm-Leach-Bliley, 15 U.S.C. § 6801, et. seq. also includes an “affirmative and continuing obligation to respect the privacy of its customers and to protect the security and confidentiality of those customers’ nonpublic personal information.” 15 U.S.C. § 6801.

18. Defendant is prohibited by the Federal Trade Commission Act (15 U.S.C. § 45) from engaging in “unfair or deceptive acts or practices in or affecting commerce.” The Federal Trade Commission has found that a company’s failure to maintain reasonable and appropriate data security for consumers’ sensitive personal information is an “unfair practice” in violation of the Federal Trade Commission Act.

19. As described below, Defendant was also required by various state laws and regulations to protect the Affected Individuals’ Personal Information.

20. In addition to their obligations under federal and state laws, Defendant owed a duty to the Affected Individuals, who entrusted it with sensitive Personal

Information, to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the Personal Information in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. Defendant owed a duty to Affected Individuals to provide reasonable security, including consistency with industry standards and requirements, and to ensure that it adequately protected the Personal Information of the Affected Individuals.

21. Defendant owed a duty to Affected Individuals, who entrusted it with sensitive Personal Information, to design, maintain, and test their computer systems to ensure that the Personal Information in Defendant's possession was adequately secured and protected.

III. Defendant's Inadequate Security Allowed for the Data Breach

22. On March 4, 2016, 21st Century announced that an unauthorized third party had breached the 21st Century Database, and thus had access to the Personal Information of the Affected Individuals which was held in the 21st Century Database.

23. 21st Century admits that the information accessed about the Affected Individuals included the Personal Information, specifically names, Social Security numbers, medical diagnoses and treatment, and insurance information. The unauthorized third party cyber-attacker has access to this Personal Information for approximately 2.2 million Affected Individuals.

IV. Defendant's Data Breach Was a Direct Result of Their Inadequate Data Security

24. Affected Individuals' Personal Information was compromised in the 21st Century Data Breach because Defendant violated its promises and legal obligations to maintain the security of the highly sensitive Personal Information that Affected Individuals entrusted to Defendant.

25. Despite their promises and legal obligations, Defendant did not provide reasonable or adequate security for Affected Individuals' Personal Information. As the creator and main operator of the 21st Century Database, 21st Century is responsible for the inadequate data security practices.

26. Defendant breached its duties to the Affected Individuals by the conduct alleged herein.

27. Defendant violated its promises and representations contained in its privacy and security notices.

28. Defendant violated its promise to comply with federal and state law to maintain the security of Affected Individuals' Personal Information, such as HIPAA.

29. Defendant violated the Gramm-Leach-Bliley Act by failing to protect the security and confidentiality of its patients' "nonpublic personal information." 15 U.S.C. § 6801.

30. Defendant violated the Federal Trade Commission Act by engaging in the "unfair practice" of failing to maintain reasonable and appropriate data security for patients' sensitive Personal Information.

V. The Affected Individuals Have Suffered and Will Suffer Substantial Harm As a Result of the Data Breach

31. The FTC defines identity theft as “a fraud committed or attempted using the identifying information of another person without authority.” The FTC describes “identifying information” as “any name or number that may be used, alone or in conjunction with any other information, to identify a specific person,” including, among other things, “[n]ame, Social Security number, date of birth, official State or government issued driver’s license or identification number, alien registration number, government passport number, employer or taxpayer identification number.”

32. Identity theft victims, particularly those exposed to medical identity theft, must spend countless hours and large amounts of money guarding against or repairing the impact to their credit and reputation. This reality was recognized in an independent study released in February 2015 by the Ponemon Institute LLC entitled “Fifth Annual Study on Medical Identity Theft”, (the “Study”).

33. With access to an individual’s Personal Information, a hacker can cause a multitude of harms to the Affected Individuals, including depleting bank accounts, obtaining a driver’s license or official identification card in a victim’s name, using a victim’s name and Social Security Number to obtain government benefits, filing a fraudulent tax return using a victim’s information, or even receive medical services and benefits. Further, loss of private and personal health care information can expose a victim to, at a minimum, loss of reputation. Personal Information is such a valuable commodity

that once the information has been compromised, criminals can trade the information on the “cyber black- market” for years.

34. The research by Ponemon, sponsored by the Medical Identity Fraud Alliance (MIFA), confirms that medical identity theft is costly and complex to resolve, and therefore it is critical for healthcare providers to take additional steps to assist victims resolve the consequences of the theft and prevent future fraud.

35. Since the study done by Ponemon in 2014, medical identity theft victim incidents increased 21.7 percent. Noting that these medical identity theft victims can suffer significant financial consequences, the Study reported that sixty-five percent (65%) of such victims in the Study had to pay an average of \$13,500 to resolve the resultant crimes.

36. The Study further found that only 10 percent (10%) of those in the study (“respondents”) reported having achieved complete satisfaction in concluding the incident. Accordingly, respondents are at risk for future theft or errors in healthcare records that could jeopardize medical treatments and diagnoses.

37. The average time spent by those respondents who successfully resolved their situation was more than 200 hours, working with their insurer or healthcare provider to make sure their personal medical credentials were secure and verifying the accuracy of their personal health information, medical invoices and claims and electronic health records. Indeed, fifty -nine percent (59%) of the respondents reported that the thief used their information to obtain healthcare services or treatments, and fifty-six percent (56%) reported that their information was used to obtain prescription pharmaceuticals or

medical equipment. Forty-five percent (45%) of respondents said that the medical identity theft incident had a negative impact on their reputation, primarily because of embarrassment due to the disclosure of sensitive personal health conditions (89 percent (89%) of those respondents). Thirty-five percent (35%) said the person committing the fraud used up their insurance benefits resulting in denial of valid insurance claims, and 31 percent said they lost their health insurance entirely as a result of the medical identity theft. Twenty-nine percent (29%) of the respondents reported that they had to make out-of-pocket payments to their health plan or insurer to restore coverage.

38. According to the Study, almost one-half of medical identity theft victims lose their healthcare coverage as a result of the identity theft, almost one-third have their insurance premiums rise, and forty percent (40%) were never able to resolve their identity theft.

39. The injuries suffered and likely to be suffered by the Affected Individuals are and will be a direct and proximate result of the 21st Century Data Breach, including:

- a) theft of their personal and financial information;
- b) loss or delay of tax refunds as a result of fraudulently filed tax returns;
- c) costs associated with the detection and prevention of identity theft and unauthorized use of their Personal Information and financial, business, banking, and other accounts;
- d) costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the 21st Century Data Breach, including finding

fraudulent charges, cancelling credit cards, purchasing credit monitoring and identity theft protection services (beyond the one-year offered by 21st Century), the imposition of withdrawal and purchase limits on compromised accounts, and the stress, nuisance, and annoyance of dealing with all issues resulting from the 21st Century Data Breach, including phishing emails and phone scams;

- e) the imminent and certain impending injury flowing from fraud and identify theft posed by their Personal Information being placed in the hands of hackers;
- f) damages to and diminution in value of their Personal Information entrusted to Defendant for the sole purpose of obtaining health care services from 21st Century;
- g) money paid to Defendant for health care services during the period of the 21st Century Data Breach because Plaintiff and Class Members would not have obtained health care services from Defendant had Defendant disclosed that it lacked adequate systems and procedures to reasonably safeguard patients' Personal Information; and
- h) overpayments to Defendant for health care services purchased, in that a portion of the amount paid by Affected Individuals to Defendant was for the costs for Defendant to take reasonable and adequate security measures to protect Affected Individuals' Personal Information, which Defendant failed to do.

40. 21st Century itself acknowledges the harm caused by the 21st Century Data Breach because it offered Affected Individuals twelve (12) months of identity theft repair and credit monitoring services. One-year of identity theft repair and credit monitoring is woefully inadequate to protect Affected Individuals from a virtual lifetime of identity theft risk and does nothing to reimburse Plaintiff and Class Members for the injuries they have already suffered.

CLASS ACTION ALLEGATIONS

A. State and Nationwide Classes

41. Pursuant to Fed. R. Civ. P. 23(b) and (c), Plaintiff assert common law claims on behalf of the following state and nationwide classes of current and former patients of 21st Century for negligence (Count I), negligence per se (Count II), negligent misrepresentation (Count III), unjust enrichment (Count IV), as well as statutory claims under Florida's consumer protection statutes (Count V).

State of Florida Class: All residents of Florida whose Personal Information was maintained on the 21st Century Database and was compromised as a result of the Data Breach announced by 21st Century on or around March 4, 2016 (the "Florida Class").

Nationwide Class: All residents of the U.S. states in which 21st Century operates whose Personal Information was maintained on the 21st Century Database and was compromised as a result of the Data Breach announced by 21st Century on or around March 4, 2016 (the "Nationwide Class").

42. Excluded from the Florida Class and the Nationwide Class (collectively the “Classes” or the “Class”) are Defendant, any entity in which Defendant has a controlling interest, any entity which has a controlling interest in Defendant, and their respective officers, directors, members, managers, legal representatives, successors, subsidiaries, and assigns. Also excluded from the Classes are any judge, justice, or judicial officer presiding over this matter and the members of their immediate families and judicial staff.

B. Certification of the Proposed Class is Appropriate

43. Each of the proposed Classes meets the requirements of Fed. R. Civ. P. 23(a), (b)(1), (b)(2), (b)(3), and (c)(4).

44. *Numerosity:* The exact number of members of the Classes is unknown to Plaintiff at this time but there are at least approximately 2.2 million individuals in all of the Classes combined, making joinder of each individual member impracticable. Ultimately, members of the Classes will be easily identified through Defendant’s records.

45. *Commonality and Predominance:* There are many questions of law and fact common to the claims of Plaintiff and the other members of the Classes, and those questions predominate over any questions that may affect individual members of the Classes. Common questions for the Classes include:

- a) Whether Defendant failed to adequately safeguard Plaintiff’s and the Classes’ Personal Information;
- b) Whether Defendant failed to protect Plaintiff’s and the Classes’ Personal Information, as promised;

- c) Whether Defendant's computer system systems and data security practices used to protect Plaintiff's and the Classes' Personal Information violated HIPAA, federal, state and local laws, or Defendant's duties;
- d) Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard Plaintiff's and the Classes' Personal Information properly and/or as promised;
- e) Whether Defendant violated federal and state consumer protection statutes, data breach and personal privacy statutes, and medical privacy statutes applicable to Plaintiff and each of the Classes;
- f) Whether Defendant acted negligently in failing to safeguard Plaintiff's and the Classes' Personal Information;
- g) Whether implied or express contracts existed between Defendant, on the one hand, and Plaintiff and the members of the each of the Classes, on the other;
- h) Whether Defendant's conduct described herein constitutes a breach of their implied or express contracts with Plaintiff and the members of each of the Classes;
- i) Whether Defendant should retain the money paid by Plaintiff and members of each of the Classes to protect their Personal Information;
- j) Whether Plaintiff and the members of the Classes are entitled to damages as a result of Defendant's wrongful conduct;

- k) Whether Plaintiff and the members of the Classes are entitled to restitution as a result of Defendant's wrongful conduct;
- l) What equitable relief is appropriate to redress Defendant's wrongful conduct; and
- m) What injunctive relief is appropriate to redress the imminent and currently ongoing harm faced by members of the Classes.

46. **Typicality:** Plaintiff's claims are typical of the claims of the members of the Classes. Plaintiff and the members of the Classes sustained damages as a result of Defendant's uniform wrongful conduct during transactions with them.

47. **Adequacy:** Plaintiff will fairly and adequately represent and protect the interests of the Classes, and has retained counsel competent and experienced in complex litigation and class actions. Plaintiff has no interests antagonistic to those of the Classes, and there are no defenses unique to Plaintiff. Plaintiff and his counsel are committed to prosecuting this action vigorously on behalf of the members of the proposed Classes, and have the financial resources to do so. Neither Plaintiff nor his counsel has any interest adverse to those of the other members of the Classes.

48. **Risks of Prosecuting Separate Actions:** This case is appropriate for certification because prosecution of separate actions would risk either inconsistent adjudications which would establish incompatible standards of conduct for the Defendant or would be dispositive of the interests of members of the proposed Classes. Furthermore, the 21st Century Database still exists, and is still vulnerable to future attacks – one standard of conduct is needed to ensure the future safety of the 21st Century Database.

49. *Policies Generally Applicable to the Classes:* This case is appropriate for certification because Defendant has acted or refused to act on grounds generally applicable to the Plaintiff and proposed Classes as a whole, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct towards members of the Classes, and making final injunctive relief appropriate with respect to the proposed Classes as a whole. Defendant's practices challenged herein apply to and affect the members of the Classes uniformly, and Plaintiff's challenge to those practices hinges on Defendant's conduct with respect to the proposed Classes as a whole, not on individual facts or law applicable only to Plaintiff.

50. *Superiority:* This case is also appropriate for certification because class proceedings are superior to all other available means of fair and efficient adjudication of the claims of Plaintiff and the members of the Classes. The injuries suffered by each individual member of the Classes are relatively small in comparison to the burden and expense of individual prosecution of the litigation necessitated by Defendant's conduct. Absent a class action, it would be virtually impossible for individual members of the Classes to obtain effective relief from Defendant. Even if members of the Classes could sustain individual litigation, it would not be preferable to a class action because individual litigation would increase the delay and expense to all parties, including the Court, and would require duplicative consideration of the common legal and factual issues presented here. By contrast, a class action presents far fewer management difficulties and provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single Court.

51. As a health care provider, Defendant is required to protect its patients' sensitive Personal Information by adopting and implementing the specific data security regulations and standards set forth under HIPAA. In addition to its implied statutory obligation, Defendant specifically promised to safeguard its patients' sensitive Personal Information in accordance with HIPAA regulations and standards through its privacy policy and patient agreements.

52. However, Defendant breached its statutory and common law obligations and express promises by maintaining its patients' sensitive Personal Information in an electronic database that lacked adequate security measures and protocols.

Defendant Violated HIPAA and Industry-Standard Data Protection Protocols

53. 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 sensitive personal information, like the Personal Information data left unguarded by Defendant. The HHS has subsequently promulgated five rules under authority of the Administrative Simplification provisions of HIPAA.

54. Defendant's data breach resulted from a combination of insufficiencies—especially pertaining to Defendant's data security relating to its patients' Personal Information—that indicate Defendant did not comply with safeguards mandated by HIPAA regulations and industry standards. Among other such insufficiencies, Defendant either failed to implement, or inadequately implemented, information security policies or procedures that protected or otherwise controlled the storage of Personal Information on

Defendant's computers. In addition, Defendant's prolonged data breach could have been prevented if Defendant had honored its obligations to its patients by implementing HIPAA mandated, industry standard policies and procedures for securely maintaining their Personal Information.

55. Defendant's security failures also include, but are not limited to, the following:

- a) Failing to maintain an adequate data security system to prevent unauthorized access to Patient Information;
- b) Failing to ensure the confidentiality and integrity of electronic protected health information it created, received, maintained, and transmitted in violation of 45 CFR 164.306(a)(1);
- c) Failing to implement policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 CFR 164.308(a)(1);
- d) 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); and
- e) Failing to design, implement, and enforce policies and procedures establishing physical and administrative safeguards to reasonably safeguard protected health information, in compliance with 45 CFR 164.530(c).

56. Even though Defendant's patients both expected and paid for the above described security measures as a part of their hospital experience (i.e., that HIPAA mandated and industry standards would be used to protect their Personal Information),

they were not implemented, which resulted in the unauthorized access of their Personal Information.

COUNT I

Negligence

(On Behalf of Nationwide and Florida Classes)

57. Plaintiff incorporates the above allegations by reference.

58. Defendant required Plaintiff and Members of the Classes to submit Personal Information in order to receive health care services and obtain insurance payments in connection therewith.

59. Defendant knew, or should have known, of the risks inherent in collecting and storing the Personal Information of Plaintiff and Members of the Classes.

60. As described above, 21st Century owed duties of care to Plaintiff and Members of the Classes whose Personal Information had been entrusted with 21st Century and was placed in the 21st Century Database due to their dealings with 21st Century.

61. Defendant breached its duties to Plaintiff and Members of the Classes by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and the Classes' Personal Information.

62. Defendant acted with wanton disregard for the security of Plaintiff and Class Members' Personal Information. Defendant knew or should have known that it had inadequate computer systems and data security practices to safeguard such information, and Defendant knew or should have known that hackers were attempting to access the Personal Information in health care databases, such as 21st Century's.

63. A “special relationship” exists between Defendant and the Plaintiff and Members of the Classes. 21st Century entered into a “special relationship” with the Plaintiff and Class Members whose Personal Information was requested, collected, and received by 21st Century, which created and maintained centralized computer systems and data security practices that were used for storage of all of 21st Century patients’ Personal Information. Thus, 21st Century also created a “special relationship” with Plaintiff and Members of the Classes whose Personal Information was placed in the 21st Century Database.

64. But for Defendant’s wrongful and negligent breach of their duties owed to Plaintiff and Members of the Classes, Plaintiff and the Members of the Classes would not have been injured.

65. The injury and harm suffered and to be suffered by Plaintiff and Members of the Classes was the reasonably foreseeable result of Defendant’s breach of its duties. Defendant knew or should have known that it was failing to meet its duties, and that Defendant’s breach would cause Plaintiff and Members of the Classes to experience the foreseeable harms associated with the exposure of their Personal Information.

66. As a direct and proximate result of Defendant’s negligent conduct, Plaintiff and Members of the Classes have suffered injury and are entitled to damages in an amount to be proven at trial.

COUNT II
Negligence Per Se
(On Behalf of the Nationwide Class)

67. Plaintiff incorporates the above allegations by reference.

68. Pursuant to the Federal Trade Commission Act (15 U.S.C. §45), Defendant 21st Century had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' Personal Information.

69. Pursuant to HIPAA (42 U.S.C. §1302d et. seq.), Defendant had a duty to implement reasonable safeguards to protect Plaintiff's and Members of the Classes' Personal Information.

70. Pursuant to the Gramm-Leach-Bliley Act (15 U.S.C. § 6801), Defendant had a duty to protect the security and confidentiality of Plaintiff's and Members of the Classes' Personal Information.

71. Pursuant to state laws in states in which 21st Century operates, 21st Century states had a duty to those respective states' Class Members to implement and maintain reasonable security procedures and practices to safeguard Plaintiff's and Class Members' Personal Information, including Florida: Fla. Stat. § 501.171(2).

72. Defendant breached its duties to Plaintiff and Class Members under the Federal Trade Commission Act (15 U.S.C. § 45), HIPAA (42 U.S.C. § 1302d et. seq.), Gramm-Leach-Bliley Act (15 U.S.C. § 6801), and the applicable state reasonable data security statutes by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' Personal Information.

73. Defendant's failure to comply with applicable federal and state laws and regulations constitutes negligence per se.

74. But for Defendant's wrongful and negligent breach of their duties owed to Plaintiff and Class Members, Plaintiff and the Class Members would not have been injured.

75. The injury and harm suffered by Plaintiff and the Class Members was the reasonably foreseeable result of Defendant's breach of its duties. Defendant knew or should have known that it was failing to meet its duties, and that Defendant's breach would cause Plaintiff and Class Members to experience the foreseeable harms associated with the exposure of their Personal Information.

76. As a direct and proximate result of Defendant's negligent conduct, Plaintiff and Class Members have suffered injury and are entitled to damages in an amount to be proven at trial.

COUNT III
Negligent Misrepresentation
(On Behalf of the Nationwide Class)

77. Plaintiff incorporates the above allegations by reference.

78. Defendant 21st Century negligently and recklessly misrepresented material facts, pertaining to the provision of health care services to Plaintiff and Class Members by representing that they would maintain adequate data privacy and security practices and procedures to safeguard Plaintiff and Class Members' Personal Information from unauthorized disclosure, release, data breaches, and theft.

79. Defendant 21st Century negligently and recklessly misrepresented material facts, pertaining to the provision of health care services to Plaintiff and Class Members by representing that they did and would comply with the requirements of relevant federal

and state laws pertaining to the privacy and security of Plaintiff's and Class Members' Personal Information.

80. In reliance upon these misrepresentations, Plaintiff and Class Members paid for health care services from Defendant.

81. Had Plaintiff and Class Members, as reasonable persons, known of Defendant's inadequate data privacy and security practices, or that Defendant was failing to comply with the requirements of federal and state laws pertaining to the privacy and security of Class Members' Personal Information, they would not have engaged Defendant to provide or paid for health care services from Defendant, and would not have entrusted their Personal Information to Defendant.

82. As direct and proximate consequence of Defendant's negligent misrepresentations, Plaintiff and Class Members have suffered the injuries alleged above.

COUNT IV
Unjust Enrichment
(On Behalf of the Nationwide Class)

83. Plaintiff incorporates the above allegations by reference.

84. Plaintiff and Class Members conferred a monetary benefit on Defendant 21st Century in the form of payment for the health care services provided to them by 21st Century.

85. 21st Century appreciated or had knowledge of the benefits conferred upon them by Plaintiff and Class Members.

86. The payment for health services that Plaintiff and Class Members paid (directly or indirectly through health insurance) to Defendant were supposed to be used

by Defendant, in part, to pay for the administrative costs of reasonable data privacy and security practices and procedures.

87. As a result of 21st Century's conduct, Plaintiff and Class Members suffered actual damages in an amount equal to the difference in value between health care services with the reasonable data privacy and security practices and procedures that Plaintiff and Class Members paid for, and the inadequate health care services without reasonable data privacy and security practices and procedures that they received.

88. Under principles of equity and good conscience, Defendant 21st Century should not be permitted to retain the money belonging to Plaintiff and Class Members because Defendant failed to implement (or adequately implement) the data privacy and security practices and procedures that Plaintiff and Class Members paid for and that were otherwise mandated by HIPAA regulations, federal, state and local laws, and industry standards.

89. 21st Century should be compelled to disgorge into a common fund for the benefit of Plaintiff and Class Members all unlawful or inequitable proceeds received by 21st Century.

90. A constructive trust should be imposed upon all unlawful or inequitable sums received by 21st Century traceable to Plaintiff and Class Members.

91. Plaintiff and Class Members have no adequate remedy at law.

COUNT V

Violations of Florida's Deceptive and Unfair Trade Practices Act

92. Plaintiff and Florida Class Members have a vested interest in the privacy, security and integrity of their Personal Information and therefore, this interest is a "thing of value" as contemplated by FDUTPA.

93. Defendant is a "person" within the meaning of the FDUTPA and, at all pertinent times, was subject to the requirements and proscriptions of the FDUTPA with respect to all of their business and trade practices described herein.

94. Plaintiff and Florida Class Members are "consumers" "likely to be damaged" by Defendant's ongoing deceptive trade practices. Defendant's unlawful conduct as described in herein, was facilitated, directed, and mandated from Defendant's headquarters to the detriment of Plaintiff and the Florida Class.

95. Defendant engaged in unfair and deceptive trade practices by holding itself out as providing a secure data environment and by actively promoting trust with patients, the consumers, which created in its patients' minds a reasonable expectation of privacy by promising that their Personal Information was and is safe, but then failed to take commercially reasonable steps to protect the Personal Information with which it is entrusted.

96. Defendant violated FDUTPA by failing to properly implement adequate, commercially reasonable security measures to protect Plaintiff's and the Florida Class'

sensitive Personal Information, as well as otherwise failing to comply with federal and state law concerning the security and safeguarding of Personal Information.

97. Defendant represents its services as having a particular standard and quality. Contrary to this representation, Defendant failed to properly implement adequate, commercially reasonable security measures to hold Personal Information in strict confidence, failed to safeguard Plaintiff's and Florida Class Members' Personal Information, failed to comply with federal and state laws concerning the security and safeguarding of Personal Information and failed to protect against the foreseeable loss and misuse of this information.

98. Plaintiff and the Florida Class have suffered and will continue to suffer ascertainable losses as a direct result of Defendant's employment of unconscionable acts or practices, and unfair or deceptive acts or practices.

99. Under FDUPTA, Plaintiff and the Florida Class are entitled to preliminary and permanent injunctive relief without proof of monetary damage, loss of profits, or intent to deceive. Plaintiff and the Florida Class seek equitable relief and to enjoin Defendant on terms that the Court considers appropriate.

100. Defendant's conduct caused and continues to cause substantial injury to Plaintiff and the Florida Class. Unless preliminary and permanent injunctive relief is granted, Plaintiff and the Florida Class will suffer harm, Plaintiff and the Florida Class Members do not have an adequate remedy at law, and the balance of the equities weighs in favor of Plaintiff and the Florida Class.

101. As a direct and proximate result of Defendant's conduct, Plaintiff and the Florida Class have suffered damages in the past and will suffer future damages, including the lost monetary value of their Personal Information, the costs associated with protecting their Personal Information now that it has been exposed, the value of time spent dealing with the breach, the loss of their right to privacy, and other damages.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of himself and the Classes, seeks the following relief:

A. An order certifying this action as a class action under Fed. R. Civ. P. 23, defining the Classes as requested herein, appointed the undersigned as Class counsel, and finding that Plaintiff is a proper representative of the Classes requested herein.

B. Awarding injunctive and other equitable relief as is necessary to protect the interests of the Classes, including (i) an order prohibiting Defendant from engaging in the wrongful and unlawful acts described herein; (ii) requiring Defendant to protect all data collected or received through the course of their business in accordance with HIPAA regulations, the Gramm-Leach Bliley Act, other federal, state and local laws, and best practices under industry standards; (iii) requiring Defendant to design, maintain, and test their computer systems to ensure that Personal Information in their possession is adequately secured and protected; (iv) requiring Defendant to disclose any future data breaches in a timely and accurate manner; (v) requiring Defendant to engage third-party security auditors 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 them to promptly correct any problems or issues detected by these auditors; (vi) requiring 21st Century to segment data by, among other things, creating firewalls and access controls so that if one area of the 21st Century network is compromised, hackers cannot gain access to other portions of 21st Century's systems; (vii) requiring Defendant to purge, delete, and destroy in a reasonably secure and timely manner Personal Information no longer necessary for their provision of services; (viii) requiring Defendant to conduct regular database scanning and securing checks; (ix) requiring Defendant to provide lifetime credit monitoring and identity theft repair services to members of the Classes; and (x) requiring Defendant to educate all Class Members about the threats they face as a result of the loss of their Personal Information to third parties, as well as steps Class Members must take to protect themselves.


C. Plaintiff also requests such actual damages, punitive damages, treble damages, statutory damages, exemplary damages, equitable relief, restitution, and disgorgement of profits as permitted or provided for under federal and state laws.

JURY DEMAND

Plaintiff demand a trial by jury on all issues so triable as a matter of right.

Dated: March 17, 2016

Respectfully submitted,


/s/ Kenneth G. Gilman

Kenneth G. Gilman

Florida Bar No. 340758

GILMAN LAW LLP

8951 Bonita Beach Road, S.E. Suite 525

Bonita Springs, FL 34135

Telephone: (239)221-8301

kgilman@gilmanlawllp.com

*Attorneys for Plaintiff and Proposed
Classes*