

**UNITED STATES DISTRICT COURT
MIDDLE DISTRICT OF FLORIDA
FORT MYERS DIVISION**

JIM BIMONTE and MARY ANN
RODRIGUEZ, individually and on behalf of
others similarly situated,

Plaintiffs,

v.

21st CENTURY ONCOLOGY, INC.; 21st
CENTURY ONCOLOGY, LLC, 21st
CENTURY ONCOLOGY MANAGEMENT
SERVICES, INC.; 21st CENTURY
ONCOLOGY SERVICES, LLC; and 21st
CENTURY ONCOLOGY HOLDINGS, INC.,

Defendants.

Case No. _____

**CLASS ACTION COMPLAINT AND
DEMAND FOR JURY TRIAL**

Plaintiffs Jim Bimonte and Mary Ann Rodriguez (“Plaintiffs”) bring this Class Action Complaint on behalf of themselves and on behalf of the proposed classes defined herein and allege as follows:

INTRODUCTION

1. On March 4, 2016, 21st Century Oncology, a nationwide network of cancer treatment centers, announced to its patients that their most sensitive personal and medical information had been compromised when an unauthorized third-party gained access to its databases. Although required by numerous state and federal laws to safeguard its patients’ confidential data with strong cybersecurity measures, 21st Century Oncology failed to comply with its legal obligations to do so. In fact, 21st Century Oncology was not even aware that its networks had been infiltrated until the Federal Bureau of Investigation (“FBI”)

gave it notice of the data breach *six* weeks after it started. As a result of 21st Century Oncology's conduct, nearly 2.2 million patients nationwide are now subject to the well-known risks and harms associated with such a breach, including identity theft, medical identity theft, and the loss of privacy in their personal and health information.

2. Accordingly, Plaintiffs Jim Bimonte and Mary Ann Rodriguez bring this putative class action alleging 21st Century Oncology has failed to adequately protect its patients' data from unauthorized access. Plaintiffs seek all available remedies at law and equity, including but not limited to damages and restitution, as well as declaratory and injunctive relief necessary to safeguard patient data from future unauthorized access and disclosures.

JURISDICTION AND VENUE

3. This Court has subject matter jurisdiction of Plaintiffs' Fair Credit Reporting Act and Declaratory Relief claims pursuant to 28 U.S.C. § 1331. This Court also has subject matter jurisdiction over Plaintiffs' state law claims pursuant to 28 U.S.C. § 1367. This Court has personal jurisdiction over 21st Century Oncology because at all relevant times, it was headquartered in and conducted (and continues to conduct) substantial business in the Middle District of Florida.

4. Venue is proper in this District under 28 U.S.C. § 1391 because 21st Century Oncology does substantial business within this District and a substantial part of the events or omissions giving rise to Plaintiffs' claims occurred within this District.

PARTIES

5. Plaintiff Jim Bimonte is a resident of Broward County, Florida.
6. Plaintiff Mary Ann Rodriguez is a resident of Palm Beach County, Florida.
7. Defendant 21st Century Oncology, Inc. is a Florida corporation with its principal place of business and headquarters at 2270 Colonial Blvd. in Fort Myers, Florida.
8. Defendant 21st Century Oncology, LLC is a Florida corporation with its principal place of business and headquarters at 2270 Colonial Blvd. in Fort Myers, Florida.
9. Defendant 21st Century Oncology Management Services, Inc. is a Florida corporation with its principal place of business and headquarters at 2270 Colonial Blvd. in Fort Myers, Florida.
10. Defendant 21st Century Oncology Services, LLC is a Florida corporation with its principal place of business and headquarters at 2270 Colonial Blvd. in Fort Myers, Florida.
11. Defendant 21st Century Oncology Holdings, Inc., is a Delaware corporation with its principal place of business and headquarters at 2270 Colonial Blvd. in Fort Myers, Florida.
12. Unless otherwise stated, all Defendants are collectively referred to herein as “21st Century Oncology” or “Defendants.” Plaintiffs are informed and allege that at all relevant times 21st Century Oncology shared common management, officers, owners, and directors, and that they carried out a joint scheme, business plan, or policy, and that acts or omissions of each are attributable to the other. Plaintiffs are informed and allege that each and every of the acts and omissions alleged herein were performed by, and/or attributable to,

all Defendants, each acting as agents and/or employees, and/or under the direction and control of each of the other Defendants, and that said acts and failures to act were within the course and scope of said agency, employment and/or direction and control.

FACTUAL BACKGROUND

A. 21st Century Oncology Provides Cancer Treatment Nationwide

13. 21st Century Oncology is a 30 year old, physician led company headquartered in Fort Myers, Florida, that bills itself as “the premier provider of cancer care services across multiple modalities.” 21st Century Oncology claims to be the largest radiation oncology provider in the United States, throughout which it operates 147 treatment centers in 17 different states. 21st Century Oncology also manages 36 treatment centers in seven countries in Latin America.

14. Throughout its treatment centers, 21st Century Oncology employs or is affiliated with over 900 physicians, including radiation oncologists and other cancer-related specialists that include urologists, hematologists, gynecologic oncologists, surgeons, and pathologists. 21st Century Oncology advertises that it maintains specialties in a number of cancer related treatments and surgeries, including those such as radiation oncology, breast cancer surgery, colorectal surgeries, and pulmonology.

15. 21st Century Oncology is managed by Dr. Daniel Dosoretz, who serves as its Chief Executive Officer. Dr. Dosoretz says that “What sets [21st Century Oncology] apart from everyone else is our relentless pursuit of great medical outcomes, the best technology, and the ability to make sure that technology and that know-how diffuses to a very wide

platform.” Defendants are also managed by Leanne M. Steward, Dr. Constantine A. Mantz, Joseph Biscardi, Frank English, James Rubenstein, and Dr. Howard Sheridan.

B. 21st Century Oncology Collects Sensitive Personal And Medical Information

16. As a direct provider of medical services, 21st Century Oncology collects and maintains possession, custody, and control of: (1) personally identifiable information (“PII”), including, without limitation, patients’ names, dates of birth, Social Security numbers, and addresses; and (2) protected health information (“PHI”), which contains PII in addition to patients’ demographic information, medical histories, prescription, diagnostic, and treatment information, test and laboratory results, insurance information, and other data collected in the normal course of providing and obtaining payment for medical services.

17. When patients begin treatment with 21st Century Oncology they complete enrollment forms and other paperwork which require them to provide an extensive amount of PII and PHI. 21st Century Oncology continues to collect and maintain its patients’ PII and PHI throughout the course of treatment and states that it is required to maintain records afterwards.

18. According to the Notice of Privacy Practices (“NOPP”) that was posted on 21st Century Oncology’s website in 2015, 21st Century Oncology creates a record of each time a patient visits a physician or receives treatment. The “record may contain [patients’] symptoms, examination and test results, diagnoses, treatment, a plan for future care or treatment, and billing-related information.” 21st Century Oncology prefaces its NOPP by stating that all of its promises regarding privacy apply to “all of the records of your care generated by your physician.”

19. Among other things, 21st Century Oncology's NOPP guarantees to patients that:

We are required by law to maintain the privacy of your protected health information, to provide you with a notice of our legal duties and privacy practices with respect to that protected health information, and to notify any affected individuals following a breach of any unsecured protected health information. We will abide by the terms of the [NOPP] currently in effect.

20. 21st Century Oncology's NOPP then provides a litany of *permissive* disclosures of PII and PHI it may undertake, such as for treatment, payment, research, and healthcare operations, which includes things such as providing information to business associates, to inform patients about possible treatment alternatives, and for conducting training programs for health care professionals. 21st Century Oncology also informs patients that it will disclose PII and PHI when otherwise *required* by law, such as to the U.S. Food and Drug Administration, to public health authorities charged with controlling diseases, to national security and intelligence agencies, and when otherwise required pursuant to a valid subpoena or court order.

C. 21st Century Oncology Is Required By Law To Protect PII And PHI

21. 21st Century Oncology is obligated by a number of state and federal laws to protect its patients' PII and PHI. Under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), and its accompanying regulations, health care providers like 21st Century Oncology are required to maintain reasonable and appropriate administrative, technical, and physical safeguards for protecting PHI, including data that is electronically stored. Among other things, 21st Century Oncology is required by HIPAA to:

- Ensure the confidentiality, integrity, and availability of all PHI it creates, receives, maintains or transmits;
- Identify and protect against reasonably anticipated threats to the security or integrity of the information;
- Protect against reasonably anticipated, impermissible uses or disclosures; and
- Ensure compliance by its workforce.¹

22. HIPAA also requires health care providers like 21st Century Oncology to preserve the integrity of PII and PHI so that it is not altered or destroyed in an unauthorized manner, and that it is only available and accessible to authorized persons. One other key component of HIPAA is that it requires health care providers to implement administrative safeguards, including ongoing risk management analyses to evaluate potential or likely risks to patients' PHI. In order to prevent the unauthorized disclosure of PHI, 21st Century Oncology is also required to implement physical and technical safeguards as part of a comprehensive data security protocol that is overseen by a chief privacy officer.

23. 21st Century Oncology is also subject to the federal laws protecting consumer data pursuant to the Fair Credit Reporting Act, 15 U.S.C. §§ 1681-1681x ("FCRA"), the Federal Trade Commission Act, 15 U.S.C. § 45 ("FTCA"), and the Gramm-Leach Bliley Act, 15 U.S.C. § 6801, *et seq.* ("GLBA").

24. The FCRA requires any business that shares data for consumer credit reporting purposes to maintain reasonable procedures designed to limit the furnishing of data to the purposes listed in the statute. 15 U.S.C. § 1681e. Under the FCRA, a "person that

¹ See <http://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/>, last accessed March 18, 2016.

receives medical information shall not disclose such information to any other person, except as necessary to carry out the purpose for which the information was initially disclosed, or as otherwise permitted by statute, regulation, or order.” 15 U.S.C. §§ 1681b(g)(4), 1681b(g)(3)(A). As disclosed in the NOPP, 21st Century Oncology collects and shares PII and PHI for purposes of collecting payment from insurers or third-party payers, subjecting it to the FCRA’s requirements to safeguard PII and PHI and limit unauthorized disclosures. Similarly, 21st Century Oncology is covered by the mandates of the FTCA, which prohibits it from unfair and deceptive conduct affecting commerce, a law that has been enforced and interpreted to include a company’s data security practices. 21st Century Oncology also maintains an obligation to “respect the privacy of its customers and to protect the security and confidentiality of those customers’ nonpublic personal information” under the GLBA.

25. The state of Florida, where 21st Century Oncology is headquartered and managed from, similarly maintains stringent legal requirements for companies that maintain electronic PII and PHI. Among other things, Florida requires 21st Century Oncology to (1) take reasonable measures to protect and secure data in electronic form containing PII; (2) take reasonable measures to dispose or destroy PII; and (3) provide notice to consumers and consumer reporting agencies subject to the FCRA when a data security incident occurs that compromises PII. Fla. Stat. § 501.171. Other states that 21st Century Oncology does business in have similar, if not stricter, requirements, for securing personal and medical information and data breach notification, including California, Kentucky, Michigan, and Washington. *See, e.g.,* Cal. Civ. Code §§ 56, *et seq.*; Cal. Civ. Code §§ 1798.80. *et seq.*; Ky.

Rev. Stat. Ann. §§ 50-7a02(a), *et seq.*; Mich. Comp. Laws Ann. §§ 445.72(1), *et seq.*; Wash. Rev. Code §§ 19.255.010(1), *et seq.*; Wash. Rev. Code §§ 70.02.045, *et seq.*

D. PHI And PII Exposure Harms Patients And Leads To Identity Theft

26. Identity theft occurs when a person’s PII is used or attempted to be used without his or her permission to commit fraud or other crimes.² Javelin Strategy & Research, a leading provider of quantitative and qualitative research, released a 2013 Identity Fraud Report, quantifying the impact of security breaches.³ According to the Javelin Report, individuals whose PII is subject to a reported security breach—such as the one at issue here—have a 25% chance of becoming a victim of identity fraud, and those who had their social security number stolen were 5 times more likely than the general public to be a fraud victim.

27. “[T]he range of privacy-related harms is more expansive than economic or physical harm or unwarranted intrusions and [] any privacy framework should recognize additional harms that might arise from unanticipated uses of data.”⁴ Furthermore, “there is significant evidence demonstrating that technological advances and the ability to combine disparate pieces of data can lead to identification of a consumer, computer or device even if the individual pieces of data do not constitute PII.”

² See Federal Trade Commission, *Warning Signs of Identity Theft*, available at (<https://www.identitytheft.gov/Warning-Signs-of-Identity-Theft>) (last visited Mar. 18, 2016).

³ See <https://www.javelinstrategy.com/press-release/more-12-million-identity-fraud-victims-2012-according-latest-javelin-strategy-research> (last visited Mar. 18, 2016).

⁴ See Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change*, at 8 (Mar. 2012), available at <http://www.ftc.gov/os/2012/03/120326privacyreport.pdf> (last visited Mar. 18, 2016).

28. Victims of identity theft are at serious risk of, and do experience, substantial losses. “Once identity thieves have your personal information, they can drain your bank account, run up charges on your credit cards, open new utility accounts, or get medical treatment on your health insurance. An identity thief can file a tax refund in your name and get your refund. In some extreme cases, a thief might even give your name to the police during an arrest.”⁵

29. Theft of medical information, such as that included in the breach here, is gravely serious: “A thief may use your name or health insurance numbers to see a doctor, get prescription drugs, file claims with your insurance provider, or get other care. If the thief’s health information is mixed with yours, your treatment, insurance and payment records, and credit report may be affected.”⁶

30. Identity thieves also use Social Security numbers to commit other types of fraud. Identity thieves use PII and PHI to open financial accounts and payment card accounts and incur charges in a victim’s name. Identity thieves also use stolen Social Security numbers to obtain false identification cards, obtain government benefits in the victim’s name, obtain jobs, and rent houses and apartments. This type of identity theft can be the most damaging because it may take some time for the victim to become aware of the theft, while in the meantime causing significant harm to the victim’s credit rating and finances.

⁵ See Federal Trade Commission, *Signs of Identity Theft*, available at <https://www.consumer.ftc.gov/articles/0271-warning-signs-identity-theft> (last visited Mar. 18, 2016).

⁶ See Federal Trade Commission, *Medical Identity Theft*, <https://www.consumer.ftc.gov/articles/0171-medical-identity-theft> (last visited Mar. 18, 2016).

Moreover, unlike other PII and PHI, Social Security numbers are incredibly difficult to change and their misuse can continue for years into the future. Victims of identity theft face substantial costs and inconvenience repairing damage to their credit records.

31. The unauthorized disclosure of a person's Social Security number can be particularly damaging because Social Security numbers cannot be easily replaced. In order to obtain a new Social Security number, a person must show evidence that someone is using the number fraudulently, as well as show that he has done all he can to fix the problems resulting from the misuse.⁷ Thus, a person whose PII and PHI has been stolen cannot obtain a new Social Security number until the damage has already been done.

32. Obtaining a new Social Security number also is not a complete remedy for identity theft. Government agencies, private businesses and credit reporting companies likely still have the person's records under the old number, so using a new number will not guarantee a fresh start. For some victims of identity theft, a new number may actually create new problems. Because prior positive credit information is not associated with the new Social Security number, it is more difficult to obtain credit due to the absence of a credit history, which can lead to higher interest rates.

33. PII and PHI is such a valuable commodity to identity thieves so that once the information has been compromised, criminals often trade the information on the "cyber black

⁷ See Social Security Administration, *Identity Theft and Your Social Security Number*, SSA Publication No. 05-10064, October 2007, ICN 46327, available at <https://www.ssa.gov/pubs/EN-05-10064.pdf> (last visited Mar. 18, 2016).

market” for a number of years.⁸ Identity thieves and other cyber criminals openly post stolen credit card numbers, Social Security numbers, and other personal financial information on various Internet websites, thereby making the information publicly available. In one study, researchers found hundreds of websites displaying stolen personal financial information. 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.”⁹

E. 21st Century Oncology Exposes Patients’ PHI And PII In Data Breach

34. On March 4, 2016, 21st Century Oncology sent a letter to its patients disclosing for the first time that it was aware of a data security breach (“Data Breach”) that compromised its patients’ PII and PHI, including their names, Social Security numbers, physicians’ names, diagnosis and treatment information, and insurance information. The Data Breach has reportedly impacted 2.2 million patients.

35. 21st Century Oncology informed its patients that it was first alerted to the Data Breach by the FBI on November 13, 2015, and that a forensics team determined the

⁸ Companies also recognize PII and PHI as an extremely valuable commodity akin to a form of personal property. See T. Soma, *et al*, *Corporate Privacy Trend: The “Value” of Personally Identifiable Information (“PII”) Equals the “Value” of Financial Assets*, 15 RICH. J.L. & TECH. 11, at *3–4 (2009).

⁹ See Stop The Hacker, *The Underground Credit Card Blackmarket*, available at <http://www.stopthehacker.com/2010/03/03/the-underground-credit-card-blackmarket/> (last visited Mar. 18, 2016).

breach occurred on or about October 3, 2015. Notably, 21st Century Oncology did not notify its patients of the data breach for nearly four months, providing cyber criminals ample time to use, sell or trade Plaintiffs' and other patients' PHI and PII without their knowledge. 21st Century Oncology's delay was especially egregious in this instance because it provided criminals with plenty of time to file false tax returns for the 2015 tax year, even though patients could have been warned about such a problem much sooner.

36. As a result of the Data Breach, 21st Century Oncology acknowledges Plaintiffs and other patients are subject to increased risk of identity fraud, and is providing impacted patients with one year of credit monitoring services through Experian ProtectMyID Alert. 21st Century Oncology expressly warned patients that they should check their medical insurance records to determine whether they have been victims of medical identity theft. 21st Century Oncology's announcement was reported the same week it announced a \$34.7 million settlement with the Department of Justice for alleged fraudulent billing for unnecessary radiation procedures. 21st Century Oncology has provided little, if any other details on the cause, nature, or extent of the Data Breach at this time.

F. 21st Century Oncology Had A Duty To Prevent The Data Breach

37. 21st Century Oncology is and remains under a duty to Plaintiffs and Class members to maintain the security and integrity of their PII and PHI. The Data Breach was a direct and proximate result of 21st Century Oncology's failure to implement and maintain appropriate and reasonable data and cybersecurity procedures and practices to safeguard and protect Plaintiffs' and Class members' (as defined below) PII and PHI from unauthorized

access, use, and disclosure, as required by various state and federal regulations, industry practices, and its agreements with patients.

38. At all times relevant herein, 21st Century Oncology also had a duty to disclose the true facts about its substandard data and cybersecurity practices, as alleged herein. 21st Century Oncology has a duty to disclose because it is in a superior position to know the true character and quality of its data and cybersecurity practices and these facts are not something that Plaintiffs and putative Class members could have discovered independently prior to purchase or obtaining medical services from 21st Century Oncology. As a result of 21st Century Oncology's material omissions about its substandard data and cybersecurity practices, it has been able to procure business from patients who may have otherwise selected privacy and security compliant physicians, or paid less for medical services. 21st Century Oncology's substandard privacy, data and cybersecurity practices were material facts actively concealed and/or not disclosed to Plaintiffs and the Class members that a reasonable person would have considered important in deciding whether or not to obtain medical services (or pay the same price for) 21st Century Oncology's services.

39. 21st Century Oncology intentionally concealed and/or failed to disclose to consumers its substandard privacy, data and cybersecurity practices as described in this Complaint for the purpose of inducing Plaintiffs and putative Class members to act thereon. Plaintiffs and the putative class members justifiably acted upon, or relied upon to their detriment, the concealed and/or non-disclosed material facts as evidenced by their obtaining medical services and treatment from 21st Century Oncology. Had Plaintiffs known of the true character and quality of 21st Century Oncology's substandard privacy, data and

cybersecurity practices, they and the putative Class members would not have purchased (or would have paid less for) 21st Century Oncology's medical services and treatment.

40. 21st Century Oncology disregarded and violated Plaintiffs' and Class members' privacy rights, and materially harmed them in the process, by not obtaining Plaintiffs' and Class members' prior written consent to disclose their PII and PHI to any other person involved in the Data Breach—as required by HIPAA and other pertinent laws, regulations, industry standards, and internal company policies.

41. 21st Century Oncology flagrantly disregarded and violated Plaintiffs' and Class members' privacy rights, and materially harmed them in the process, by failing to establish and implement appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of Plaintiffs' and Class members' PII and PHI, and to protect against reasonably foreseeable threats to the security or integrity of such information. 21st Century Oncology's security deficiencies allowed unauthorized individuals to access, remove from its premises, transport, disclose, and compromise the PII and PHI of 2.2 million individuals—including Plaintiffs and Class members.

42. 21st Century Oncology's wrongful actions and inaction directly and proximately caused the theft and dissemination into the public domain of Plaintiffs' and Class Members' PII and PHI without their knowledge, authorization, and consent. As a direct and proximate result of 21st Century Oncology's wrongful actions and inactions and the resulting Data Breach, Plaintiffs and Class members have suffered, and will continue to suffer, economic damages and other actual harm including, without limitation: (i) the untimely and inadequate notification of the Data Breach; (ii) improper disclosure of their PII

and PHI; (iii) loss of privacy; (iv) out-of-pocket expenses reasonably incurred to remedy or mitigate the effects of identity theft, identity fraud, and medical fraud or to mitigate and avert the increased risk of identity theft, identity fraud, and medical fraud pressed upon them by the Data Breach; (v) the value of their time reasonably spent mitigating the effects of identity theft, identity fraud, and medical fraud or to mitigate or avert the increased risk of identity theft, identity fraud, and medical fraud; (vi) deprivation of the value of their PII and PHI, for which there is a well-established national and international market; (vii) the payments (or some portion thereof) for medical services and treatment paid to the Defendants; and/or (viii) rights they possess under FCRA or other statutes—for which they are entitled to compensation.

43. As a direct and proximate result of 21st Century Oncology’s wrongful actions and inaction and the resulting Data Breach, Plaintiffs and Class Members will now be required to take the time and effort to mitigate the actual and potential impact of the Data Breach on their lives including, *inter alia*, placing “freezes” and “alerts” with the credit reporting agencies, closing or modifying financial accounts, and closely reviewing and monitoring their credit reports, accounts, and explanations of benefits from insurers for unauthorized activity. Because Plaintiffs’ and Class members’ Social Security numbers were stolen and compromised, as well as their medical information, they also now face a significantly heightened risk of identity theft, identity fraud, and medical fraud.

44. As a direct and proximate result of 21st Century Oncology’s wrongful actions and inaction and the resulting Data Breach, unauthorized third parties now have Plaintiffs’ and Class members’ PII and PHI. As such, Plaintiffs and Class members have been deprived

of the value of their PII and PHI.¹⁰ It is reported that “medical records hold an average black market value of \$50 per record.”¹¹ Because in the course of treatment health care providers often share information regarding the medical history of patients, fraudulent use of PHI by imposters to obtain healthcare can also lead to misdiagnosis, errant prescriptions of medications, and severe health consequences for the victims of medical fraud.

45. As a direct and proximate result of 21st Century Oncology’s failure to properly safeguard and protect Plaintiffs’ and Class Members’ PII and PHI, including, *inter alia*, failing to secure its networks, computers, and databases, violating standard industry practices and protocols (including encryption, segregation, penetration testing, intrusion detection, etc.) for protecting PII and PHI, Plaintiffs’ and Class members’ privacy has been (and will continue to be) invaded and their rights violated. Their compromised PII and PHI was private and sensitive in nature and was left inadequately protected. Defendants’ wrongful actions and inactions and the resulting Data Breach have placed Plaintiffs and Class Members at an imminent, immediate, and continuing increased risk of harm from identity theft, identity fraud, and medical fraud.

46. Notwithstanding 21st Century Oncology’s wrongful actions and inactions and the resulting Data Breach, 21st Century Oncology has offered one year of credit monitoring

¹⁰ See, e.g., John T. Soma, J. Zachary Courson, John Cadkin, *Corporate Privacy Trend: The “Value” of Personally Identifiable Information (“PII”) Equals the “Value” of Financial Assets*, 15 RICH. J.L. & TECH. 11, at *3–4 (2009) (“PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.”) (citations omitted).

¹¹ Pamela Louis Dolan, *Health Data Breaches Usually Aren’t Accidents Anymore* (July 29, 2013), available at <http://www.amednews.com/article/20130729/business/130729953/4/> (last visited Mar. 18, 2016).

and identity theft protection services through Experian's ProtectMyId Alert. This offer is insufficient given that it does not address many categories of damages being sought. Even if fraud is detected, a person still must place "freezes" and "alerts" with the other two credit bureaus (TransUnion and Equifax), close or modify financial accounts, and closely review and monitor their credit reports, accounts, and explanations of benefits from insurers for unauthorized activity. Additionally, the PII and PHI could be held by criminals and used to commit fraud after the one year of credit monitoring and identity theft protection is up.

47. As a direct and proximate cause of 21st Century Oncology's misconduct, Plaintiffs and the putative class members have suffered actual damages, 21st Century Oncology has been unjustly enriched, and Plaintiffs and class members are entitled to appropriate relief. 21st Century Oncology's conduct has been and is malicious, wanton and/or reckless and/or shows a reckless indifference to the interests and rights of others.

PLAINTIFFS' EXPERIENCES

48. Plaintiff Jim Bimonte is a resident of Broward County, Florida. Plaintiff Bimonte paid for medical services from 21st Century Oncology. On or about March 4, 2016, Plaintiff Bimonte was notified via letter that 21st Century Oncology compromised his PII and PHI in the Data Breach, including his name, Social Security number, physicians' names, diagnosis and treatment information, and insurance information.

49. Plaintiff Mary Ann Rodriguez is a resident of Palm Beach County, Florida. Plaintiff Rodriguez paid for medical services from 21st Century Oncology. On or about March 4, 2016, Plaintiff Rodriguez was notified via letter that 21st Century Oncology

compromised her PII and PHI in the Data Breach, including her name, Social Security number, physicians' names, diagnosis and treatment information, and insurance information.

CLASS ACTION ALLEGATIONS

50. Plaintiffs bring this suit as class action pursuant to Rule 23 of the Federal Rules of Civil Procedure on behalf of themselves and all members of the following class:

All persons whose PII and/or PHI was compromised in the Data Breach announced by 21st Century Oncology on or about March 4, 2016.

51. Plaintiffs also bring claims in this suit as class action pursuant to Rule 23 of the Federal Rules of Civil Procedure on behalf of themselves and all members of the following Florida Sub-class:

All persons in Florida whose PII and/or PHI was compromised in the Data Breach announced by 21st Century Oncology on or about March 4, 2016.

52. Excluded from the Class and Florida Sub-class (collectively "Class" or "Classes") are: (1) any Judge or Magistrate presiding over this action and members of their families; (2) 21st Century Oncology, 21st Century Oncology's subsidiaries, parents, successors, predecessors, and any entity in which 21st Century Oncology has a controlling interest, and its current or former employees, officers, and directors; (3) counsel for Plaintiffs and 21st Century Oncology; and (4) legal representatives, successors, or assigns of any such excluded persons.

53. The Classes meet all of the criteria required by Federal Civil Rule 23(a).

54. **Numerosity:** The Class members are so numerous that joinder of all members is impracticable. Though the exact number and identities of Class members are

unknown at this time, but are reported to be approximately 2.2 million. The identities of Class members are ascertainable through Defendants' records, Class members' records, publication notice, self-identification, and other means.

55. **Commonality:** Common questions of law and fact exist as to all Class members. These common questions of law or fact predominate over any questions affecting only individual members of the Classes. Common questions include, but are not limited to, the following:

- (a) Whether 21st Century Oncology violated state and federal laws by failing to properly store, secure, and dispose of Plaintiffs' and Class members' PII and PHI;
- (b) Whether 21st Century Oncology failed to employ reasonable and adequate data and cybersecurity measures in compliance with applicable state and federal regulations;
- (c) Whether 21st Century Oncology acted willfully, recklessly, or negligently with regard to securing Plaintiffs' and Class members' PII and PHI;
- (d) How the Data Breach occurred;
- (e) Whether 21st Century Oncology failed to timely notify Plaintiffs and Class members of the Data Breach;
- (f) Whether Plaintiffs and Class members are entitled to restitution, damages, compensation, or other monetary relief; and

- (g) Whether Plaintiffs and Class members are entitled to injunctive and declaratory relief necessary to secure their PII and PHI from further intrusion and exposure.

56. Common sources of evidence may also be used to demonstrate 21st Century Oncology's unlawful conduct on a class-wide basis, including, but not limited to documents and testimony about its data and cybersecurity measures (or lack thereof); testing and other methods that can prove 21st Century Oncology's data and cybersecurity systems have been or remain inadequate; documents and testimony about the source, cause, and extent of the Data Breach; and documents and testimony about any remedial efforts undertaken as a result of the Data Breach.

57. **Typicality:** Plaintiffs' claims are typical of the claims of the respective Classes they seek to represent, in that the named Plaintiffs and all members of the proposed Classes have suffered similar injuries as a result of the same practices alleged herein. Plaintiffs have no interests adverse to the interests of the other members of the Classes.

58. **Adequacy:** Plaintiffs will fairly and adequately protect the interests of the Classes, and have retained attorneys well experienced in class actions and complex litigation as their counsel, including cases alleging consumer protection and data privacy claims arising from medical data breaches.

59. The Classes also satisfy the criteria for certification under Federal Civil Rule 23(b) and 23(c). Among other things, Plaintiffs aver that the prosecution of separate actions by the individual members of the proposed classes would create a risk of inconsistent or varying adjudication which would establish incompatible standards of conduct for 21st

Century Oncology; that the prosecution of separate actions by individual class members would create a risk of adjudications with respect to them which would, as a practical matter, be dispositive of the interests of other class members not parties to the adjudications, or substantially impair or impede their ability to protect their interests; that 21st Century Oncology has acted or refused to act on grounds that apply generally to the proposed classes, thereby making final injunctive relief or declaratory relief described herein appropriate with respect to the proposed classes as a whole; that questions of law or fact common to the Classes predominate over any questions affecting only individual members and that class action treatment is superior to other available methods for the fair and efficient adjudication of the controversy which is the subject of this action. Plaintiffs also aver that certification of one or more subclasses or issues may be appropriate for certification under Federal Civil Rule 23(c). Plaintiffs further state that the interests of judicial economy will be served by concentrating litigation concerning these claims in this Court, and that the management of the Classes will not be difficult.

60. Plaintiffs and other members of the Classes have suffered injury, harm, and damages as a result of 21st Century Oncology's unlawful and wrongful conduct. Absent a class action, 21st Century Oncology will continue to maintain Class members' PHI and PII that could be subject to future breaches due to lax or non-existent cybersecurity measures, and such unlawful and improper conduct should not go remedied. Absent a class action, the members of the Class will not be able to effectively litigate these claims and will suffer further harm and losses, as 21st Century Oncology will be allowed to continue such conduct with impunity and benefit from its unlawful conduct.

CLAIMS FOR RELIEF

COUNT I

**Willful Violation of the Fair Credit Reporting Act,
15 U.S.C. §§ 1681-1681x**

61. Plaintiffs incorporate all preceding paragraphs as fully set forth herein.

Plaintiffs' FCRA claim is behalf of the Classes set forth above.

62. One of the fundamental purposes of the FCRA is to protect consumers' privacy. 15 U.S.C. § 1681(a). Protecting consumers' privacy involves adopting reasonable procedures to keep sensitive information confidential. 15 U.S.C. § 1681(b).

63. The FCRA defines a "consumer reporting agency" as:

[A]ny person, which, for monetary fees, dues, or on a cooperative nonprofit basis, regularly engages in whole or in part in the practice of assembling or evaluating consumer credit information or other information or consumers for the purpose of furnishing consumer reports to third parties, and which uses any means or facility of interstate commerce for the purpose of preparing or furnishing consumer reports.

15 U.S.C. § 1681a(f).

64. The FCRA defines a "consumer report" as:

[A]ny written, oral, or other communication of any information by a consumer reporting agency bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living which is used or expected to be used or collected in whole or in part for the purpose of establishing the consumer's eligibility for (A) credit or insurance to be used primarily for personal, family, or household purposes; (B) employment purposes; or (C) any other purpose authorized under 15 U.S.C. § 16881(b).

65. 21st Century Oncology regularly assembles consumer information including, among other things, insurance policy information, such as names, dates of birth, type of loss,

and amount paid for claims submitted by an insured; and a description of insured items.

21st Century Oncology also regularly utilizes interstate commerce to furnish such information on consumers to third parties.

66. Plaintiffs' and Class members' PII and PHI constitute consumer reports under FCRA, because this information bears on, among other things, their credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, physical and mental medical conditions, and mode of living, and is used or collected, in whole or in part, for the purpose of establishing Plaintiffs' and other Class members' eligibility for insurance to be used primarily for personal, family, or household purposes, and establishing rates for same.

67. The FCRA requires the adoption of reasonable procedures with regard to, *inter alia*, the confidentiality and proper utilization of personal and insurance information. 15 U.S.C. § 1681(b). FCRA also requires that consumer reporting agencies "maintain reasonable procedures designed to . . . limit the furnishing of consumer reports to the purposes listed under section 1681b of this title." 15 U.S.C. § 1681e.

68. 21st Century Oncology failed to adopt and maintain these and other reasonable procedures designed to limit the furnishing of consumer reports to the purposes listed under the FCRA, 15 U.S.C. § 1681b. Among other things, 21st Century Oncology employed substandard or non-existent data and cybersecurity protocols such as segregation, access controls, password protection, encryption, intrusion detection, secure destruction of unnecessary data, and penetration testing. 21st Century Oncology's failure to employ these reasonable administrative, technical and physical safeguards led to the Data Breach.

69. The FCRA defines “medical information” as:

[I]nformation or data, whether oral or recorded, in any form or medium, created by or derived from a health care provider or the consumer, that relates to—(A) the past, present, or future physical, mental, or behavioral health or condition of an individual; (B) the provision of health care to an individual; or (C) the payment for the provision of health care to an individual.

15 U.S.C. § 1681(a)(i).

70. FCRA specifically protects medical information; restricting its dissemination to limited instances. *See, e.g.*, 15 U.S.C. §§ 1681a(d)(3); 1681b(g); 1681c(a)(6).

71. Plaintiffs’ and Class members’ PHI affected by the Data Breach constitutes medical information as defined by FCRA. Their PHI included enrollment and clinical information, lab and test results, diagnoses, and treating information from medical professionals which relate to the provision of health care and past, present, or future physical, mental, or behavioral health or condition of an individual under FCRA’s definition of medical information. 15 U.S.C. § 1681a(i).

72. Under the FCRA, a “person that receives medication information shall not disclose such information to any other person, except as necessary to carry out the purpose for which the information was initially disclosed, or as otherwise permitted by statute, regulation, or order.” 15 U.S.C. §§1681(g)(4), 1681b(g)(3)(A).

73. 21st Century Oncology’s failure to adequately protect and safeguard Plaintiffs’ and Class members’ PII and PHI resulted in the disclosure of such information to one or more third-parties in violation of FCRA because such disclosure was not necessary to carry out the purposes for which 21st Century Oncology received the information, nor was it permitted by statute, regulation or order.

74. 21st Century Oncology's violations of the FCRA, as set forth above, were willful or, at the very least, reckless, constituting willfulness. A number of high-profile data breaches targeting health providers and insurers, including one involving 80 million health insurance subscribers of Anthem in early 2015 has put all medical providers and insurers on sufficient notice of the high interest cyber criminals have in obtaining health information, Social Security numbers, and 21st Century Oncology knew or should have known that insurance information can be sold, traded, or used to obtain illegal benefits and services and otherwise commit fraud.

75. As a direct and proximate result of 21st Century Oncology's willful or reckless failure to adopt and maintain reasonable procedures to limit the furnishing and disclosures of Plaintiffs' and Class members' PII and PHI to the purposes listed in the statute, Plaintiffs' and Class members' PII and PHI was disclosed and disseminated to unauthorized third-parties, compromised, and stolen. Plaintiffs and Class members have suffered injury and harm, and will continue to suffer injury and harm because of 21st Century Oncology's conduct.

76. As a further direct or proximate result of 21st Century Oncology's willful or reckless FCRA violations, as described above, Plaintiffs and Class members were (and continue to be) injured and have suffered (and will continue to suffer) the harms and damages described in this Complaint.

77. Accordingly, Plaintiffs and Class members are entitled to compensation for their actual damages in an amount to be determined at trial or statutory damages of not less than \$100, and not more than \$1,000, each, as well as attorneys' fees, punitive damages,

litigation expenses and costs, pursuant to 15 U.S.C. § 1681n(a). Plaintiffs also seek injunctive relief enjoining the above described wrongful acts and practices of the 21st Century Oncology and requiring 21st Century Oncology to employ and maintain industry accepted standards for data management and security, including, but not limited to proper segregation, access controls, password protection, encryption, intrusion detection, secure destruction of unnecessary data, and penetration testing.

COUNT II
Negligent Violation of the FCRA

78. Plaintiffs reallege each and every allegation contained above, and incorporate by reference all other paragraphs of this Complaint as if fully set forth herein. Plaintiffs bring this claim on behalf of the Classes set forth above.

79. 21st Century Oncology negligently failed to adopt and maintain reasonable procedures designed to limit the furnishing of consumer reports to the purposes listed under 15 U.S.C. § 1681b.

80. Plaintiffs' and Class members' PII and PHI was wrongly disclosed and disseminated to unauthorized third-parties and the public as a direct and foreseeable result of 21st Century Oncology's failure to adopt and maintain such reasonable procedures.

81. 21st Century Oncology disclosed medical information of Plaintiffs' and Class members to one or more third-parties in violation of the FCRA because such disclosure was not necessary to carry out the purpose for which 21st Century Oncology received the information, nor was it permitted by statute, regulation, or order.

82. As a direct and proximate result of 21st Century Oncology's negligent violations of the FCRA, as described above, Plaintiffs' and Class members' PII and PHI was

made accessible to unauthorized third-parties in the public domain, compromised, and stolen. Plaintiffs have suffered harm and injury, including a loss of privacy, as a result of 21st Century Oncology's negligent FCRA violations.

83. As a further direct or proximate result of 21st Century Oncology's negligent violations of the FCRA, Plaintiffs and Class members were and continue to be injured and have suffered (and will suffer) the damages and harms as they deal with the fallout from the Data Breach for the foreseeable future. Accordingly, Plaintiffs are entitled to compensation for their actual damages, as well as attorneys' fees, litigation expenses, and costs, pursuant to 15 U.S.C. § 1681o. Plaintiffs also seek injunctive relief enjoining the above described wrongful acts and practices of the 21st Century Oncology and requiring 21st Century Oncology to employ and maintain industry accepted standards for data management and security, including, but not limited to proper segregation, access controls, password protection, encryption, intrusion detection, secure destruction of unnecessary data, and penetration testing.

COUNT III
Violation of Florida Deceptive and Unfair Trade Practices Act,
Fla. Stat. §§ 501.201, *et seq.*

84. Plaintiffs reallege each and every allegation contained above, and incorporate by reference all other paragraphs of this Complaint as if fully set forth herein. Plaintiffs bring this claim on behalf of the Classes set forth above, or alternatively, on behalf of the Florida Sub-class.

85. This cause of action is brought pursuant to the Florida Deceptive and Unfair Trade Practices Act ("FDUTPA"). Fla. Stat. §§ 501.201, *et seq.* The express purpose of the

FDUPTA is to “protect the consuming public . . . from those who engage in unfair methods of competition, or unconscionable, deceptive, or unfair acts or practices in the conduct of any trade or commerce.” Fla. Stat. § 501.202(2).

86. 21st Century Oncology’s sale of goods and medical services at issue in this cause are “consumer transaction[s]” within the scope of the FDUTPA. Fla. Stat. §§ 501.201-501.213. Plaintiffs are “consumer[s]” as defined by the FDUTPA. Fla. Stat. § 501.203. 21st Century Oncology is engaged in trade or commerce within the meaning of the FDUTPA.

87. The FDUTPA declares as unlawful “unfair methods of competition, unconscionable acts or practices, and unfair or deceptive acts or practices in the conduct of any trade or commerce.” Fla. Stat. § 501.204(1).

88. The FDUPTA provides that “due consideration be given to the interpretations of the Federal Trade Commission and the federal courts relating to Section 5(a)(1) of the Trade Commission Act.” Fla. Stat. § 501.204(2). 21st Century Oncology’s unfair and deceptive practices are likely to mislead -- and have misled -- the consumer acting reasonably under the circumstances. Fla. Stat. § 500.04; 21 U.S.C. § 343. As set forth above, 21st Century Oncology’s Data Breach was a result of its substandard data and cybersecurity practices in violation of the FCRA, HIPAA, the FTCA, the GLBA, and state law as set forth above.

89. Pursuant to the FCRA, HIPAA (42 U.S.C. § 1302d *et seq.*), the FTCA, the GLBA, and Florida law (Fla. Stat. § 501.171), 21st Century Oncology was required by law to maintain adequate and reasonable data and cybersecurity measures to maintain the security

and privacy of Plaintiffs' and Class members' PII and PHI. 21st Century Oncology was also under an obligation expressly under Florida law, where 21st Century Oncology is headquartered and managed, to adequately protect Plaintiffs' and Class members' electronic PII and PHI. Among other things, Florida requires 21st Century Oncology to (1) take reasonable measures to protect and secure data in electronic form containing PII; (2) take reasonable measures to dispose or destroy PII; and (3) provide notice to consumers and consumer reporting agencies subject to the FCRA when a data security incident occurs that compromises PII. Fla. Stat. §§ 501.171.

90. 21st Century Oncology has violated the FDUPTA by engaging in the unfair and deceptive practices described above, which offend public policies and are immoral, unethical, unscrupulous and substantially injurious to consumers. At all times material herein, 21st Century Oncology has failed to maintain adequate and reasonable data and cybersecurity protocols for Plaintiffs' and Class members PII and PHI in violation of state and federal laws and its own privacy practices and policies. 21st Century Oncology has also failed to take reasonable measures to destroy or dispose of PII and PHI and timely notify its patients of the Data Breach in violation of Florida law.

91. Plaintiffs have standing to pursue this claim because they has been injured by virtue of suffering a loss of privacy, money and/or property as a result of the wrongful conduct alleged herein. Plaintiffs would not have purchased 21st Century Oncology's goods and services (or paid as much) had they known the truth about 21st Century Oncology's substandard and shoddy data and cybersecurity measures. Moreover, 21st Century Oncology will continue to maintain Plaintiffs' and Class members' PII and PHI for the indefinite

future, giving them a strong interest in ensuring such data is protected with state of the art, industry standards to prevent future Data Breaches. As a direct result of 21st Century Oncology's actions and omissions of material facts, Plaintiffs and Class members did not obtain the value of the goods and services for which they paid; were induced to pay for (or pay more for) medical goods and services that they otherwise would not have; and lost their ability to make informed and reasoned decisions about their medical treatment.

92. The damages suffered by Plaintiffs and Class members were directly and proximately caused by the deceptive, misleading and unfair practices of 21st Century Oncology, as described above.

93. Plaintiffs and Class members seek declaratory judgment that 21st Century Oncology's data security practices were not reasonable or adequate and caused the Data Breach under the FDUTPA, as well as injunctive relief enjoining the above described wrongful acts and practices of the 21st Century Oncology and requiring 21st Century Oncology to employ and maintain industry accepted standards for data management and security, including, but not limited to proper segregation, access controls, password protection, encryption, intrusion detection, secure destruction of unnecessary data, and penetration testing. Fla. Stat. § 501.211(1).

94. Additionally, Plaintiffs and Class members make claims for actual damages, attorney's fees and costs. Fla. Stat. §§ 501.2105, 501.211(2).

COUNT IV
Negligence

95. Plaintiffs reallege each and every allegation contained above, and incorporate by reference all other paragraphs of this Complaint as if fully set forth herein. Plaintiffs

bring this claim on behalf of the Classes set forth above, or alternatively, on behalf of the Florida Sub-class.

96. 21st Century Oncology had a duty to exercise reasonable care and protect and secure Plaintiffs' and Class members' PII and PHI.

97. Through its acts and omissions, 21st Century Oncology violated its duty to use reasonable care to protect and secure Plaintiffs' and Class members' PII and PHI by employing substandard or non-existent data and cybersecurity protocols.

98. It was reasonably foreseeable, particularly given legal mandates governing health data protection and the growing number of data breaches of health information, that the failure to reasonably protect and secure Plaintiffs' and Class members' PII and PHI would result in an unauthorized third-party gaining access to 21st Century Oncology's networks, databases, and computers that stored or contained Plaintiffs' and Class members' PII and PHI.

99. Plaintiffs' and Class members' PII and PHI constitute personal property that was stolen due to 21st Century Oncology's negligence, resulting in harm, injury and damages to Plaintiffs and Class members.

100. 21st Century Oncology's negligence directly and proximately caused the unauthorized access and disclosure of Plaintiffs' and Class members' unencrypted PII and PHI and Plaintiffs and Class Members have suffered and will continue to suffer damages as a result of 21st Century Oncology's conduct. Plaintiffs and Class members seek damages and other relief as a result of 21st Century Oncology's negligence.

COUNT V
Negligence *Per Se*

101. Plaintiffs reallege each and every allegation contained above, and incorporate by reference all other paragraphs of this Complaint as if fully set forth herein. Plaintiffs bring this claim on behalf of the Classes set forth above, or alternatively, on behalf of the Florida Sub-class.

102. Pursuant to the FCRA, HIPAA (42 U.S.C. § 1302d *et seq.*), the FTCA, the GLBA, and Florida law (Fla. Stat. § 501.171), 21st Century Oncology was required by law to maintain adequate and reasonable data and cybersecurity measures to maintain the security and privacy of Plaintiffs' and Class members' PII and PHI.

103. 21st Century Oncology breached its duties by failing to employ industry standard data and cybersecurity measures to gain compliance with those laws, including, but not limited to proper segregation, access controls, password protection, encryption, intrusion detection, secure destruction of unnecessary data, and penetration testing.

104. It was reasonably foreseeable, particularly given the growing number of data breaches of health information, that the failure to reasonably protect and secure Plaintiffs' and Class members' PII and PHI in compliance with applicable laws would result in an unauthorized third-party gaining access to 21st Century Oncology's networks, databases, and computers that stored or contained Plaintiffs' and Class members' PII and PHI.

105. Plaintiffs' and Class members' PII and PHI constitute personal property that was stolen due to 21st Century Oncology's negligence, resulting in harm, injury and damages to Plaintiffs and Class members.

106. 21st Century Oncology's conduct in violation of applicable laws directly and proximately caused the unauthorized access and disclosure of Plaintiffs' and Class members' unencrypted PII and PHI and Plaintiffs and Class Members have suffered and will continue to suffer damages as a result of 21st Century Oncology's conduct. Plaintiffs and Class members seek damages and other relief as a result of 21st Century Oncology's negligence.

COUNT VI
Breach of Contract

107. Plaintiffs reallege each and every allegation contained above, and incorporate by reference all other paragraphs of this Complaint as if fully set forth herein. Plaintiffs bring this claim on behalf of the Classes set forth above, or alternatively, on behalf of the Florida Sub-class.

108. 21st Century Oncology provides medical services to Plaintiffs' and Class members pursuant to the terms of its contracts, including the NOPP, which all were a party to. As consideration, Plaintiffs and Class members paid money to 21st Century Oncology and/or their insurers for medical services. Accordingly, Plaintiffs and Class members paid 21st Century Oncology to securely maintain and store their PII and PHI. 21st Century Oncology violated its contracts, including but not limited to the NOPP, by failing to employ reasonable and adequate security measures to secure Plaintiffs' and Class members' PII and PHI and by disclosing it for purposes not required or permitted under the contracts.

109. Plaintiffs and Class members have been damaged by 21st Century Oncology's conduct, including by paying for data and cybersecurity protection that they did not receive, as well as by incurring the harms and injuries arising from the Data Breach now and in the future.

COUNT VIII
Invasion of Privacy

110. Plaintiffs reallege each and every allegation contained above, and incorporate by reference all other paragraphs of this Complaint as if fully set forth herein. Plaintiffs bring this claim on behalf of the Classes set forth above, or alternatively, on behalf of the Florida Sub-class.

111. Plaintiffs and Class members maintain a privacy interest in their PII and PHI, which is private, confidential information that is also protected from disclosure by applicable laws set forth above.

112. 21st Century Oncology's disclosure of Plaintiffs' and Class members' PII and PHI to unauthorized third-parties as a result of its failure to adequately secure and safeguard their PII and PHI is offensive to a reasonable person. 21st Century Oncology's disclosure of Plaintiffs' and Class members' PII and PHI to unauthorized third-parties permitted the physical and electronic intrusion into Plaintiffs' and Class members' private quarters where their PII and PHI was stored, and disclosed private facts about their health into the public domain.

113. Plaintiffs and Class members have been damaged by 21st Century Oncology's conduct, including by paying for data and cybersecurity protection that they did not receive, as well as by incurring the harms and injuries arising from the Data Breach now and in the future.

COUNT IX
Unjust Enrichment

114. Plaintiffs reallege each and every allegation contained above, and incorporate by reference all other paragraphs of this Complaint as if fully set forth herein. Plaintiffs bring this claim on behalf of the Classes set forth above, or alternatively, on behalf of the Florida Sub-class.

115. Plaintiffs and Class members conferred a benefit on 21st Century Oncology by paying for data and cybersecurity procedures to protect their PII and PHI that they did not receive.

116. 21st Century Oncology has retained the benefits of its unlawful conduct including the amounts received for data and cybersecurity practices that it did not provide. Due to 21st Century Oncology's conduct alleged herein, it would be unjust and inequitable under the circumstances for 21st Century Oncology to be permitted to retain the benefit of its wrongful conduct.

117. Plaintiffs and the Class Members are entitled to full refunds, restitution and/or damages from 21st Century Oncology and/or an order of this Court proportionally disgorging all profits, benefits, and other compensation obtained by 21st Century Oncology from its wrongful conduct. If necessary, the establishment of a constructive trust from which the Plaintiffs and Class members may seek restitution or compensation may be created.

118. Additionally, Plaintiffs and the Florida Sub-class Members may not have an adequate remedy at law against 21st Century Oncology, and accordingly plead this claim for unjust enrichment in addition to or, in the alternative to, other claims pleaded herein.

COUNT X
Declaratory Relief, 28 U.S.C. § 2201

119. Plaintiffs reallege each and every allegation contained above, and incorporate by reference all other paragraphs of this Complaint as if fully set forth herein. Plaintiffs bring this claim on behalf of the Classes set forth above.

120. An actual controversy has arisen and now exists between Plaintiffs and the putative Classes on the one hand, and 21st Century Oncology on the other, concerning 21st Century Oncology's failure to protect Plaintiffs' and Class members' PII and PHI in accordance with applicable state and federal regulations and the agreements between the parties. Plaintiffs and the Class members contend that 21st Century Oncology failed to maintain adequate and reasonable safeguards to protect their PII and PHI while on the other hand, 21st Century Oncology contends it has complied with applicable state and federal regulations and its agreements with Plaintiffs and Class members to protect their PII and PHI.

121. Accordingly, Plaintiffs are entitled to and seek a judicial determination of whether 21st Century Oncology has performed, and is performing, its data and cybersecurity practices obligations necessary to protect and safeguard Plaintiffs' and Class members' PII and PHI from further unauthorized, access, use, and disclosure, or insecure disposal.

122. A judicial determination of the rights and responsibilities of the parties over 21st Century Oncology's data security practices is necessary and appropriate at this time so (1) that the rights of the Plaintiffs and the Classes may be determined with certainty for purposes of resolving this action; and (2) and so that the Parties will have an understanding

of 21st Century Oncology's obligations in the future given its continued legal obligations and continued relationships with Plaintiffs and Class members.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs on their own and behalf of all others similarly situated, prays for relief as follows:

- A. For an Order certifying this case as a class action pursuant to Federal Civil Rule 23, appointing Plaintiffs as Class Representatives of their respective Classes, and the undersigned as Class Counsel;
- B. Awarding monetary, punitive and actual damages and/or restitution, as appropriate;
- C. Awarding declaratory and injunctive relief as permitted by law or equity to assure that the Class and Florida Sub-class has an effective remedy, including enjoining 21st Century Oncology from continuing the unlawful practices as set forth above;
- D. Prejudgment interest to the extent allowed by the law;
- E. Awarding all costs, experts' fees and attorneys' fees, expenses and costs of prosecuting this action; and
- F. Such other and further relief as the Court may deem just and proper.

JURY DEMAND

Plaintiffs request a trial by jury on behalf of themselves and all similarly-situated persons pursuant to Federal Rule of Civil Procedure 38.

DATED: March 22, 2016

WITES & KAPETAN, P.A.



/s/ Marc A. Wites
Marc A. Wites, Trial Counsel
Fla. Bar No. 24783
mwites@wklawyers.com
Chad R. Robinson
Fla. Bar No. 56922
crobinson@wklawyers.com
4400 North Federal Highway
Lighthouse Point, FL 33064
Tel: 954.526.2729
Fax: 954-354-0205

KAPLAN FOX & KILSHEIMER LLP

Laurence D. King (to be admitted *pro hac vice*)
Linda M. Fong (to be admitted *pro hac vice*)
Matthew George (to be admitted *pro hac vice*)
350 Sansome Street, Suite 400
San Francisco, CA 94104
Telephone: (415) 772-4700
Facsimile: (415) 772-4707
Email: lking@kaplanfox.com
lfong@kaplanfox.com
mgeorge@kaplanfox.com

Attorneys for Plaintiffs