

FILED

UNITED STATES DISTRICT COURT  
MIDDLE DISTRICT OF FLORIDA  
FORT MYERS DIVISION

2016 SEP -9 PM 1:54

U.S. DISTRICT COURT  
MIDDLE DISTRICT OF FLORIDA  
FORT MYERS

VENETA DELUCCHI and BRADLEY  
BERNIUS, individually and on behalf of all  
others similarly situated.

Plaintiffs,

v.

21<sup>ST</sup> CENTURY ONCOLOGY HOLDINGS,  
INC.,

Defendant.

CASE NO. \_\_\_\_\_

CLASS ACTION COMPLAINT

JURY TRIAL DEMAND

2:16-cv-695-FEM-99 CM

**TABLE OF CONTENTS**

I. INTRODUCTION ..... 1

II. NATURE OF THE ACTION ..... 1

III. JURISDICTION ..... 5

IV. PARTIES ..... 5

    A. Plaintiff Veneta Delucchi..... 5

    B. Plaintiff Bradley Bernius ..... 7

    C. Defendant 21<sup>st</sup> Century Oncology ..... 7

V. FACTUAL ALLEGATIONS ..... 8

    A. The Data Breach and 21<sup>st</sup> Century Oncology’s Insufficient and Delayed Response..... 8

    B. 21<sup>st</sup> Century Oncology’s Acknowledged Duty to Keep PII Private ..... 10

    C. 21<sup>st</sup> Century Oncology’s Knowledge that Thieves Seek the PII Entrusted to It..... 10

        1. The 2011-2012 Patient PII Data Breach ..... 10

        2. The increased threat to healthcare companies ..... 11

        3. The FBI’s highly publicized warning to healthcare companies..... 11

    D. 21<sup>st</sup> Century Oncology’s Marked History of Prioritizing Profit Over Patients..... 12

        1. The 2008-2012 unnecessary testing of patients ..... 13

        2. The 2009-2015 additional unnecessary testing of patients ..... 14

        3. 21<sup>st</sup> Century Oncology Scuttles Its December 10, 2013 Confidential Initial Public Offering ..... 15

    E. 21<sup>st</sup> Century Oncology’s Continued Prioritization of Profits Over Patients Injures Data Breach Victims ..... 17

        1. The obfuscation of key facts about the Data Breach ..... 17

2.	The risk of identity theft is a major concern to Data Breach victims.....	18
3.	The offered “remedy” is inadequate .....	20
a.	The offered remedies have required Data Breach victims to expend ongoing precious time containing their compromised PII.....	20
b.	Thieves will likely use Data Breach victim’s PII to hurt them far longer than a year .....	21
(i)	Compromised Social Security numbers have long-term value to thieves and long-term consequences to Data Breach victims.....	22
(ii)	Compromised medical information has even greater long-term value to thieves and consequences to Data Breach victims.....	23
4.	The delayed disclosure further harmed Data Breach victims .....	24
F.	21 <sup>st</sup> Century Oncology’s Priorities Have Caused Plaintiffs’ Most Sensitive PII to Be Compromised, Increasing Their Current and Ongoing Suffering .....	27
1.	Plaintiff Veneta Delucchi.....	27
2.	Plaintiff Bradley Bernius .....	28
VI.	CLASS ACTION ALLEGATIONS .....	28
VII.	CAUSES OF ACTION .....	31
	COUNT I Negligence .....	31
	COUNT II Breach of Implied Covenant of Good Faith and Fair Dealing .....	37
	COUNT III Violation of Florida Deceptive and Unfair Trade Practices Act Fla. Stat. § 501.201, <i>et seq.</i> .....	39
	COUNT IV Violation of the California Confidentiality of Medical Information Act Cal. Civ. Code § 56, <i>et seq.</i> (On behalf of the California Subclass).....	41

COUNT V Violations of the Customer Records Act Cal. Civ. Code §  
1798.81.5, *et seq.* (On behalf of the California Subclass) ..... 45

COUNT VII Unjust Enrichment..... 48

VIII. PRAYER FOR RELIEF ..... 50

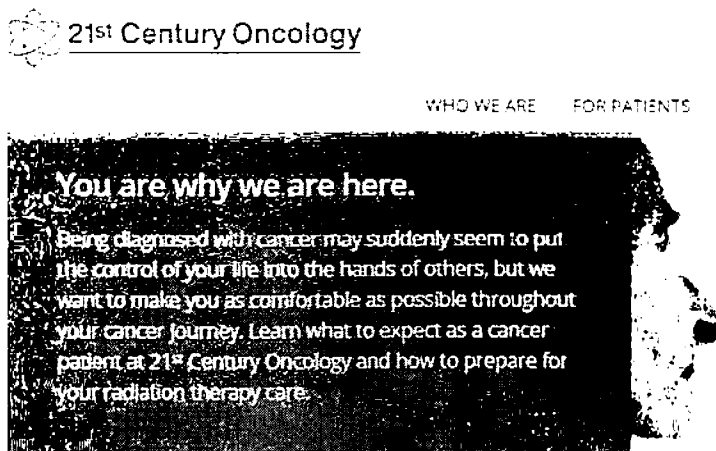
IX. JURY TRIAL DEMAND ..... 50

## I. INTRODUCTION

Plaintiffs Veneta Delucchi and Bradley Bernius, individually and on behalf of all others similarly situated, file this Class Action Complaint against 21<sup>st</sup> Century Oncology Holdings, Inc. (“Defendant” or “21<sup>st</sup> Century Oncology”), and allege as follows based on personal knowledge, the investigation of their counsel, and information and belief.

## II. NATURE OF THE ACTION

1. As any oncology patient, survivor, or loved one can attest—and 21<sup>st</sup> Century Oncology recognizes on its website<sup>1</sup>—medical challenges are stressful and difficult and a cancer diagnosis can seem to put one’s life out of control:



2. The last thing patients dealing with potentially deadly illnesses need is further harm and stress caused by the insecurity of their most private data and how it may be used by thieves.

---

<sup>1</sup> 21<sup>st</sup> Century, *What to Expect as a Cancer Patient*, <https://www.21co.com/radiation-therapy/what-to-expect> (last visited Mar. 18, 2016).

3. But that is exactly what victims of the 21<sup>st</sup> Century Oncology data breach are enduring nationwide after thieves hacked into 21<sup>st</sup> Century Oncology's provider database on or around October 3, 2015 (the "Data Breach"). While more than 2.2 million 21<sup>st</sup> Century Oncology victims were seeking and/or paying for medical care from the company, thieves were hard at work stealing and using their hard-to-change Social Security numbers and highly sensitive medical information for more than five months without their knowledge. 21<sup>st</sup> Century Oncology apparently failed to detect the Data Breach until the Federal Bureau of Investigation ("FBI") notified it of the massive breach more than a month later, on November 13, 2015.<sup>2</sup> The Data Breach resulted in the disclosure of private and highly sensitive information including names, Social Security numbers, physician's names, medical diagnoses, treatment information, and insurance information ("PII").<sup>3</sup>

4. 21<sup>st</sup> Century Oncology's lax security practices allowed the Data Breach to occur, endangering the financial, medical, and emotional well-being of millions of victims for the rest of their already-burdened lives. The Data Breach has exacerbated victims' already life-altering circumstances, including by (a) adding to their already heightened financial obligations by placing them at increased risk of fraudulent charges; and/or (b) complicating diagnosis, prognosis, and treatment for their severe medical conditions by placing them at increased risk of having inaccurate medical information in their files.

5. Making matters worse, 21<sup>st</sup> Century Oncology is not a name known to all Data Breach victims. In fact, some Data Breach victims were shocked and alarmed to learn that 21<sup>st</sup>

---

<sup>2</sup> 21<sup>st</sup> Century, *Notice to Patients Regarding Security Incident* (Mar. 4, 2016), <https://www.21co.com/securityincident> (last visited Mar. 18, 2016).

<sup>3</sup> *Id.*

Century Oncology had access to their PII at all, much less had lost control of their PII and allowed it to be compromised by an unauthorized third party who could further distribute their private and sensitive PII to anyone and everyone, including identity thieves.

6. Indeed, 21<sup>st</sup> Century Oncology has acknowledged in the Notice of Privacy Practices that is posted on its website that it is “required by law to maintain the privacy of your protected health information, to provide you with 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.”<sup>4</sup> It also represented that it would abide by these obligations. 21<sup>st</sup> Century Oncology failed to live up to its own promises, much less those required by law.

7. Contrary to its promises to help patients improve the quality of their lives through secure data practices, 21<sup>st</sup> Century Oncology’s conduct has been a direct cause of the ongoing harm to these Data Breach victims who will continue to experience harm and data insecurity for the indefinite future.

8. Specifically, 21<sup>st</sup> Century Oncology failed to maintain reasonable and/or adequate security measures to protect Data Breach victims’ PII from unauthorized access and disclosure, which lacked, at a minimum: (1) security measures designed to prevent this attack even though 21<sup>st</sup> Century Oncology has suffered from at least one previous data breach, and knew or should have known that it was a prized target for hackers; and (2) security protocols

---

<sup>4</sup> 21<sup>st</sup> Century, *Notice of Privacy Practices* (Mar. 26, 2013), <https://www.21.co.com/~/media/files/revise%20npp%20for%2021c%20web%20site.pdf>.

to promptly detect the Data Breach and removal of data from its provider database pertaining to 2.2 million patients.

9. Moreover, while 21<sup>st</sup> Century Oncology reportedly had months to figure out how to protect and minimize harm to victims of the Data Breach, its response has been slapdash and ineffective. First, 21<sup>st</sup> Century Oncology harmed victims through delayed notification. Adding insult to injury, it then offered only one year of credit monitoring and identity theft insurance, which is wholly insufficient. Credit monitoring and identity theft insurance do not protect against identity theft. Rather, they force Data Breach victims first to actually experience the stress of theft, and then to spend the time to undo financial injury inflicted by identity thieves who seek to use their compromised PII for financial gain.

10. In addition, credit monitoring fails to remedy the potentially life-threatening injury to Data Breach victims inflicted by identity thieves who seek to use the victims' compromised information to obtain medical care, thereby placing the thieves' inaccurate information on innocent victims' medical records in the process. This harm is particularly dangerous for oncology patients.

11. Furthermore, thieves with access to Data Breach victims' compromised PII can use their Social Security numbers indefinitely because, unlike credit and financial accounts, these numbers are difficult to change. In addition, medical identity theft can continue to harm Data Breach victims indefinitely because this information is often shared amongst numerous providers.

12. Plaintiffs are Data Breach victims and bring this proposed class action lawsuit on behalf of themselves and all other persons whose PII has been compromised as a result of



the Data Breach. They seek injunctive relief requiring 21<sup>st</sup> Century Oncology to implement and maintain security practices to comply with regulations designed to prevent and remedy these and other potential data breaches, as well as restitution, damages, and other relief as the Court may order. Plaintiffs and other Data Breach victims will have to remain vigilant for the rest of their lives to combat potential identity theft. Despite the best efforts of Plaintiffs and Data Breach victims, this most sensitive personal data can never be made private again.

### **III. JURISDICTION**

13. This Court has jurisdiction over this Action pursuant to 28 U.S.C. § 1332(d) because the amount in controversy exceeds \$5 million, exclusive of interest and costs, 21<sup>st</sup> Century Oncology does business nationwide in 17 states, and members of the proposed class are citizens of different states than 21<sup>st</sup> Century Oncology.

14. This Court has personal jurisdiction over 21<sup>st</sup> Century Oncology because 21<sup>st</sup> Century Oncology maintains its headquarters and principal executive and administrative offices in Florida and it has sufficient minimum contacts with Florida.

15. Venue is proper in this district under 28 U.S.C. § 1391(b) because 21<sup>st</sup> Century Oncology resides in this district and a substantial part of the events or omissions giving rise to Plaintiffs' claims occurred in this district.

### **IV. PARTIES**

#### **A. Plaintiff Veneta Delucchi**

16. Plaintiff Veneta Delucchi is a citizen and resident of California.

17. Plaintiff Delucchi has received and paid for medical care in California.

18. On information and belief, some of Plaintiff Delucchi's medical care has been provided by one or more employees and/or affiliates of 21<sup>st</sup> Century Oncology in California prior to the Data Breach.

19. On information and belief, Plaintiff Delucchi had her private and sensitive medical information and other PII collected, stored, maintained, and/or generated by employees and/or affiliates of 21<sup>st</sup> Century Oncology in California prior to the Data Breach, including, based on information and belief, her name, Social Security number, physician's name, diagnosis and treatment information, and insurance information.

20. Plaintiff Delucchi reasonably expected the confidentiality of her private and sensitive medical information and other PII entrusted to employees and/or affiliates of 21<sup>st</sup> Century Oncology would be kept securely.

21. Plaintiff Delucchi did not authorize 21<sup>st</sup> Century Oncology to release her private and sensitive medical information and other PII to anyone other than her treating oncologist during her course of treatment at a 21<sup>st</sup> Century Oncology affiliate, or thereafter.

22. In March 2016, Plaintiff Delucchi received a notification from 21<sup>st</sup> Century Oncology that her private and sensitive medical and other PII was compromised due to the Data Breach and that an unauthorized third party "may have accessed" a 21<sup>st</sup> Century Oncology database "which contained information that may have included your name, Social Security number, physician's name, diagnosis and treatment information, and insurance information."

23. Plaintiff Delucchi has been injured as a result of the Data Breach. Prior to receiving the Data Breach notification letter, Plaintiff Delucchi was unaware that 21<sup>st</sup> Century

Oncology disclosed or released any of her medical information or other PII to anyone without her written authorization, or that any of her medical information or other PII was unsecure.

**B. Plaintiff Bradley Bernius**

24. Plaintiff Bradley Bernius resides and is domiciled in the State of California.

25. From March 2011 through approximately March 2012, Plaintiff Bernius received cancer treatment from 21<sup>st</sup> Century Oncology in its Redding, California facility.

26. At the start of his treatment, Plaintiff Bernius provided 21<sup>st</sup> Century Oncology his PII, including his address, date of birth, past medical history, and medical conditions. Plaintiff Bernius also promptly updated his address with 21<sup>st</sup> Century Oncology after each change of residence.

27. Plaintiff Bernius, however, has not received a letter notifying him of the Data Breach. Nonetheless, he reasonably believes he is one of the approximately 2.2 million victims of the Data Breach because he provided his medical information and other PII to 21<sup>st</sup> Century Oncology since March 2011. Additionally, when he and his caretaker called 21<sup>st</sup> Century Oncology in April 2016, 21<sup>st</sup> Century Oncology confirmed that Plaintiff Bernius' PII was contained in the database compromised in the Data Breach.

28. Plaintiff Bernius has been injured as a result of the Data Breach, including spending numerous hours investigating the Data Breach, enrolling in credit monitoring service, and reviewing his credit reports and financial statements for fraudulent activity.

**C. Defendant 21<sup>st</sup> Century Oncology**

29. Defendant 21<sup>st</sup> Century Oncology is a corporation organized under the laws of Delaware and maintains its principal executive and administrative offices in Fort Myers,

Florida. 21<sup>st</sup> Century Oncology, through its wholly-owned subsidiaries, is a leading global, physician-led provider of integrated cancer care services.

30. 21<sup>st</sup> Century Oncology provides a full spectrum of cancer care services by employing and affiliating with physicians in their related specialties, which enables 21<sup>st</sup> Century Oncology to collaborate across its physician base, integrate services and payments for related medical needs, and to disseminate its medical practices on a broad scale.

31. 21<sup>st</sup> Century Oncology operates the largest integrated network of cancer treatment centers and affiliated physicians in the world. As of December 31, 2014, the 21<sup>st</sup> Century Oncology network was comprised of approximately 794 community-based physicians in the fields of radiation oncology, medical oncology, breast, gynecological and general surgery, urology and primary care.

32. 21<sup>st</sup> Century Oncology cancer treatment centers in the United States are operated predominantly under the *21<sup>st</sup> Century Oncology* brand and are present in 17 states: Alabama, Arizona, California, Florida, Indiana, Kentucky, Maryland, Massachusetts, Michigan, Nevada, New Jersey, New York, North Carolina, Rhode Island, South Carolina, Washington and West Virginia.

## V. FACTUAL ALLEGATIONS

### A. **The Data Breach and 21<sup>st</sup> Century Oncology's Insufficient and Delayed Response**

33. On November 13, 2015, the FBI advised 21<sup>st</sup> Century Oncology that "patient information was illegally obtained by a third party may have gained access to a 21<sup>st</sup> Century

Oncology database.”<sup>5</sup> According to 21<sup>st</sup> Century Oncology, once it was informed of the Data Breach, it hired a leading forensics firm to aid in the investigation as well as “assess their systems and bolster security.”<sup>6</sup> As a result of that investigation, 21<sup>st</sup> Century Oncology determined that the intruder may have accessed the database on October 3, 2015, nearly six weeks before 21<sup>st</sup> Century Oncology was aware of the intrusion, and five months before notifying Plaintiffs and the Class.

34. The PII accessed included highly sensitive information such as names, Social Security numbers, physicians’ names, diagnoses and treatment information, as well as insurance information.

35. On March 4, 2016, 21<sup>st</sup> Century Oncology filed a United States Securities and Exchange Commission (“SEC”) Form 8-K<sup>7</sup> that publicly disclosed the Data Breach, stating:

The FBI asked that 21<sup>st</sup> Century delay notification or public announcement of the incident until today so as to not interfere with its investigation. Now that law enforcement’s request for delay has ended, the company is notifying patients as quickly as possible.

36. As explained further below, 21<sup>st</sup> Century Oncology is promising Data Breach victims—as it has done in the past—that it will implement additional security measures and internal security protocols to help prevent similar instances in the future. It is also offering, as it has done in the past, one year of credit monitoring.

---

<sup>5</sup> 21<sup>st</sup> Century, *Letter to Office of the Attorney General of New Hampshire* (March 4, 2016), <http://doj.nh.gov/consumer/security-breaches/documents/21st-century-oncology-20160304.pdf>, attached as exhibit A.

<sup>6</sup> *Id.*

<sup>7</sup> 21<sup>st</sup> Century SEC Form 8-K (Mar. 4, 2016), <https://www.21co.com/investors/sec-filings>.

37. However, 21<sup>st</sup> Century Oncology is not learning from past mistakes and its offer for one year of monitoring and identity theft insurance is woefully insufficient given the nature of the PII accessed.

**B. 21<sup>st</sup> Century Oncology's Acknowledged Duty to Keep PII Private**

38. 21<sup>st</sup> Century Oncology has acknowledged since March 26, 2013 in its Notice of Privacy Practices<sup>8</sup> that it is required by law to maintain the privacy of the Data Breach victims' PII and notify them if their PII was compromised in compliance with applicable law:

**Our Responsibilities**

We are required by law to maintain the privacy of your protected health information, to provide you with 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 notice currently in effect.

It failed to do so.

**C. 21<sup>st</sup> Century Oncology's Knowledge that Thieves Seek the PII Entrusted to It**

**1. The 2011-2012 Patient PII Data Breach**

39. Unfortunately, due to the highly sensitive nature of the data it handles, 21<sup>st</sup> Century Oncology is no stranger to data breaches.

40. On or about May 15, 2013, federal law enforcement officials informed 21<sup>st</sup> Century Oncology that it was indicting one of its employees for having improperly accessed patient PII over the course of almost ten months, between October 11, 2011 and August 8, 2012. This 21<sup>st</sup> Century Oncology employee provided patient PII to a third party who then used patient names, Social Security numbers, and dates of birth to file fraudulent claims for

---

<sup>8</sup> 21<sup>st</sup> Century, *Notice of Privacy Practices* (Mar. 26, 2013), <https://www.21.co.com>.

tax refunds. As with the Data Breach, 21<sup>st</sup> Century Oncology failed to detect the 2011-2012 data breach.

41. When 21<sup>st</sup> Century Oncology later notified the Maryland Attorney General of the 2011-2012 data breach on or about July 10, 2013, 21<sup>st</sup> Century Oncology had not yet concluded its own internal investigation into how the employee was able to access this information.

42. Ultimately, 21<sup>st</sup> Century Oncology offered victims affected by the 2011-2012 data breach one year of credit monitoring and an assurance that “protecting our patients’ personal information is a priority at 21<sup>st</sup> Century Oncology... and we take any potential misuse of our patients’ private health information very seriously.”<sup>9</sup>

43. In the ensuing years, however, 21<sup>st</sup> Century Oncology did not carry through with its promises and only obtained—and thereby put at risk—far more patient data.

**2. The increased threat to healthcare companies**

44. According to cybersecurity company SANS Institute, healthcare providers and health insurance companies are regular targets of cyber-attacks, and are particularly vulnerable to them.<sup>10</sup>

**3. The FBI’s highly publicized warning to healthcare companies**

45. The FBI’s cyber division warned health care systems in April 2014 that cyber-attacks were likely to increase after January 2015, when healthcare companies were required

---

<sup>9</sup> 21<sup>st</sup> Century, *Letter to Office of the Attorney General of Maryland* (July 10, 2013), <https://www.oag.state.md.us/idtheft/Breach%20Notices/2013/itu-230673.pdf>, attached as exhibit B.

<sup>10</sup> SANS Institute, *Health Care Cyberthreat Report: Widespread Compromises Detected, Compliance Nightmare on Horizon* (Feb. 2014), <http://www.sans.org/reading-room/whitepapers/analyst/health-care-cyberthreat-report-widespread-compromises-detected-compliance-nightmare-horizon-34735>.

to switch from using paper medical records to electronic records. The FBI noted that healthcare companies were more susceptible to cyber-attacks because of the data they possessed, making future attacks likely.<sup>11</sup> This report was highly publicized in 2014, and was reported by various news agencies.<sup>12</sup>

46. Yet, 21<sup>st</sup> Century Oncology appears not to have heeded these warnings to reasonably and adequately secure this private and highly sensitive PII, as demonstrated by its failure to detect the Data Breach until the FBI (again) reported it to 21<sup>st</sup> Century Oncology. As Twistlock's chief strategy officer Chenxi Wang told *ESecurity Planet*:

The fact that many of these breaches are reported by the FBI, rather than discovered by the company that holds the data, speaks to the heart of the problem—many organizations do not have sufficient technical expertise and capabilities in place to protect data and respond in a timely manner in the event of a breach[.]<sup>13</sup>

**D. 21<sup>st</sup> Century Oncology's Marked History of Prioritizing Profit Over Patients**

47. The Data Breach should be viewed in the context of the corporate culture in which it arose. Contrary to its stated commitment on its website to provide “compassionate” cancer care to patients,<sup>14</sup> 21<sup>st</sup> Century Oncology, through its wholly-owned subsidiaries, has been subjecting patients to a variety of unnecessary medical testing for at least seven years.

---

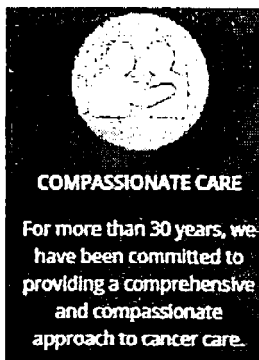
<sup>11</sup> FBI Cyber Division Private Industry Notification (April 8, 2014), <https://info.publicintelligence.net/FBI-HealthCareCyberIntrusions.pdf>.

<sup>12</sup> Finkle, *Exclusive: FBI Warns Healthcare Sector Vulnerable to Cyber Attacks*, Reuters (April 23, 2014), <http://www.reuters.com/article/2014/04/23/us-cybersecurity-healthcare-fbi-exclusividUSBREA3M1Q920140423>.

<sup>13</sup> Jeff Goldman, *21st Century Oncology Notifies 2.2 Million Patients of Data Breach* (Mar. 11, 2016), <http://www.esecurityplanet.com/network-security/21st-century-oncology-notifies-2.2-million-patients-of-data-breach.html>.

<sup>14</sup> 21<sup>st</sup> Century, Home Page, <https://www.21co.com> (last visited Mar. 18, 2016).





**1. The 2008-2012 unnecessary testing of patients**

48. On March 25, 2013—two months before the FBI informed 21<sup>st</sup> Century Oncology of the 2011-2012 data breach—a medical assistant filed a whistleblower suit against a 21<sup>st</sup> Century Oncology subsidiary alleging a scheme to subject patients to unnecessary tests in order to fraudulently collect money from federal health care programs from 2008 through 2012.<sup>15</sup>

49. In the words of Special Agent in Charge Shimon Richmond of the Department of Health and Human Services Office of Inspector General: “These tests were ordered to increase profits, not improve the health care of patients.”<sup>16</sup>

50. On December 16, 2015—one month after the FBI informed 21<sup>st</sup> Century Oncology of the recently disclosed Data Breach—21<sup>st</sup> Century Oncology filed an SEC Form 8-K that announced that it was settling the whistleblower suit for \$19.75 million.<sup>17</sup>

---

<sup>15</sup> *United States, State of Florida, ex rel. Mariela Barnes, v. Dr. David Spellberg, 21 Century Oncology and Naples Urology Associates*, Civil Action No. 2:13-cv-228-FtM-99DNF (M.D. Fla.).

<sup>16</sup> Don Browne, *21st Century Oncology Paying \$19 Million Settlement In False Billing Case*, Southwest Florida Online (Dec. 18, 2015), <http://swflorida.blogspot.com/2015/12/21st-century-oncology-paying-19-million.html>.

<sup>17</sup> 21<sup>st</sup> Century SEC Form 8-k (Dec. 16, 2015), <https://www.21co.com/investors/sec-filings>.

**2. The 2009-2015 additional unnecessary testing of patients**

51. On October 19, 2015—less than a month before the FBI informed 21<sup>st</sup> Century Oncology of the instant Data Breach—a doctor filed a whistleblower suit against a 21<sup>st</sup> Century Oncology subsidiary alleging a scheme to subject patients to four categories of unnecessary tests in order to fraudulently collect money from federal health care programs from 2009 through 2014.<sup>18</sup>

52. “The company prioritized profit over medical counsel,” said David L. Scher, counsel for the whistleblowing doctor.<sup>19</sup>

53. Jason Mehta, Assistant U.S. Attorney agreed, stating: “When medical decision-making is influenced by significant financial incentives, patients suffer—and, in this case, patients and taxpayers were bilked for a test of questionable validity that the government contends, in some cases, offered no value or meaning to any healthcare practitioners.”<sup>20</sup>

54. On March 9, 2016—days after publicly disclosing the Data Breach—21<sup>st</sup> Century Oncology filed an SEC Form 8-K that announced that it was settling the second whistleblower suit for \$34.7 million.<sup>21</sup>

---

<sup>18</sup> *United States ex rel. Joseph Ting v. 21<sup>st</sup> Century Oncology and South Florida Radiation Oncology*, Civil Action No. 3:14-cv-723-Jax-J32JRK (M.D. Fla).

<sup>19</sup> Patricia Brooks, *Medicare Fraud Whistleblower Represented By The Employment Law Group® Law Firm Wins \$34.7 Million Settlement In Case Against 21st Century Oncology*, PR Newswire (Mar. 8, 2016), <http://www.prnewswire.com/news-releases/medicare-fraud-whistleblower-represented-by-the-employment-law-group-law-firm-wins-347-million-settlement-in-case-against-21st-century-oncology-300232646.html>.

<sup>20</sup> *Id.*

<sup>21</sup> 21<sup>st</sup> Century SEC Form 8-K (Mar. 9, 2016), <https://www.21co.com/investors/sec-filings>.

**3. 21<sup>st</sup> Century Oncology Scuttles Its December 10, 2013 Confidential Initial Public Offering**

55. When 21<sup>st</sup> Century Oncology realized that it was going to have to answer for years of subjecting patients to unnecessary tests for profit, it quietly began efforts to shift its liability for these misdeeds by confidentially filing an initial public offering (“IPO”) on December 10, 2013.<sup>22</sup>

56. According to equity analyst Kris Tuttle, 21<sup>st</sup> Century Oncology pitched a fairly simple growth by acquisition story to investors:

The investment story is fairly simple - cancer is a large and growing problem that requires treatment. We are the biggest and best option and will continue to grow by acquisition.<sup>23</sup>

57. 21<sup>st</sup> Century Oncology, postponed its IPO on May 22, 2014, however, citing poor market conditions.<sup>24</sup>

58. Analyst Tuttle noted that the reason 21<sup>st</sup> Century Oncology was only getting limited interest in the IPO in May 2014 was that its balance sheet included debt it was looking to restructure.

59. If the deal failed to get done, analyst Tuttle suggested that the company go back to the drawing board and focus the growth and the story:

If the deal fails to get done we’d send this company back to the drawing board and focus the growth and the story more on technology-driven improvements in transparency, cost efficiency and higher quality of care. Right now the positioning is

---

<sup>22</sup> Renaissance Capital, *21st Century Oncology postpones IPO*, Nasdaq (May 22, 2014), <https://www.nasdaq.com/article/21st-century-oncology-postpones-ipo-cm355444>.

<sup>23</sup> Kris Tuttle, *Tepid Demand for 21st Century Oncology IPO*, IPO Candy (May 22, 2014), <https://ipocandy.com/2014/05/tepid-demand-for-21st-century-oncology-ipo/>.

<sup>24</sup> Renaissance Capital, *21st Century Oncology postpones IPO*, Nasdaq (May 22, 2014), <https://www.nasdaq.com/article/21st-century-oncology-postpones-ipo-cm355444>.

“we’re a little better than a hospital-based center on average and we can buy up centers in a fragmented market.”<sup>25</sup>

60. 21<sup>st</sup> Century Oncology appears to have taken the “form” of analyst Tuttle’s suggestion to heart, stating in its annual report for the year ended December 31, 2014:

Given the changing healthcare landscape, increased focus on lower cost, higher quality care and the potential for value-based reimbursement, we built a complete and integrated cancer care platform to better meet the needs of patients, physicians and payers.<sup>26</sup>

61. Ultimately, however, 21<sup>st</sup> Century Oncology was forced to disclose to investors in its December 18, 2015 8-K filing that it was settling the first whistleblower’s allegations that 21<sup>st</sup> Century Oncology had been subjecting its patients to unnecessary testing for short-sighted profits for \$19.75 million—which was incompatible with the “substance” of analyst Tuttle’s suggestion.<sup>27</sup>

62. The last nail in the coffin for 21<sup>st</sup> Century Oncology’s proposed IPO occurred two weeks later, on January 5, 2016, when the *Wall Street Journal* reported that 21<sup>st</sup> Century Oncology had withdrawn its long-delayed IPO after recently agreeing “to pay \$19.75 million to settle civil allegations by the Justice Department that its doctors performed the test on Medicare patients more often than medically necessary” and also talking with the Justice Department about setting “a second investigation into its use of a radiation-oncology procedure.”<sup>28</sup>

---

<sup>25</sup> Kris Tuttle, *Tepid Demand for 21st Century Oncology IPO*, IPO Candy (May 22, 2014), <https://ipocandy.com/2014/05/tepid-demand-for-21st-century-oncology-ipo/>.

<sup>26</sup> 21<sup>st</sup> Century SEC Form 10-K (Mar. 27, 2015), <https://www.21co.com/investors/sec-filings>.

<sup>27</sup> 21<sup>st</sup> Century SEC Form 8-k (Dec. 16, 2015), <https://www.21co.com/investors/sec-filings>.

<sup>28</sup> Chelsey Dulaney and John Carreyrou, *21st Century Oncology Withdraws IPO: Cancer-care giant was recently embroiled in Medicare billing investigation*, Wall St. J. (Jan. 5, 2016), <http://www.wsj.com/articles/21st-century-oncology-withdraws-ipo-1452033845>.

**E. 21<sup>st</sup> Century Oncology's Continued Prioritization of Profits Over Patients Injures Data Breach Victims**

**1. The obfuscation of key facts about the Data Breach**

63. Although 21<sup>st</sup> Century Oncology failed to detect two data breaches, placed profits over patient care for years, and notified victims of the Data Breach five months after it occurred, 21<sup>st</sup> Century Oncology asserts that it can now be trusted to act in their interests and protect their PII. Again, its actions suggest otherwise.

64. Despite having had months to prepare its notification to Data Breach victims, 21<sup>st</sup> Century Oncology informed Data Breach victims only that an intruder “may have accessed its database that contained patient names, Social Security numbers, physicians’ names, diagnoses and treatment information, and insurance information,” and suggested that Data Breach Victims should be comforted because *it* found “no evidence that patients’ medical records were accessed.”<sup>29</sup>

65. James Chappell, Digital Shadows’ Chief Technology Officer and co-founder, expressed surprise at 21<sup>st</sup> Century Oncology’s callous and calculating description of the scope of this breach, particularly given the known life circumstances of these Data Breach victims, stating:

The circumstances in these patients’ lives were already pretty tough ... I’m surprised 21<sup>st</sup> Century Oncology weren’t better stewards of their patients’ data given their circumstances.<sup>30</sup>

---

<sup>29</sup> 21<sup>st</sup> Century SEC Form 8-K (Mar. 4, 2016), <https://www.21co.com/investors/sec-filings>.

<sup>30</sup> Tom Spring, *Cancer Clinic Warns 2.2 Million Patients of Records Breach*, (Mar. 8, 2016), <https://threatpost.com/cancer-clinic-warns-2-2-million-patients-of-records-breach/116668/> (last accessed Mar. 18, 2016).

66. Ted Harrington, executive partner with Independent Security Evaluators, likewise believes that 21<sup>st</sup> Century Oncology's response is off-base, stating:

21<sup>st</sup> Century Oncology's response really misses the mark. ... patient names, Social Security numbers and other data ... are some of the most important aspects of the medical record.<sup>31</sup>

67. Senior HHS advisor Rachel Seeger has similarly been quoted in the media emphasizing that names and Social Security Numbers are protected under the Health Insurance Portability and Accountability Act ("HIPAA")—even if no specific diagnostic or treatment information is disclosed as it was here:

The personally identifiable information that HIPAA-covered health plans maintain on enrollees and members — including names and Social Security Numbers — is protected under HIPAA, even if no specific diagnostic or treatment information is disclosed.<sup>32</sup>

**2. The risk of identity theft is a major concern to Data Breach victims**

68. Hackers steal PII in order to view, mine, exploit, use and/or profit from it. Most hackers view, mine, and package the hacked PII for sale on black market sites to identity thieves<sup>33</sup> who intend to exploit, use and/or profit from it. Hackers have also sometimes been

---

<sup>31</sup> Paul Benjou, *Negligence is the Cancer of CyberCrime*. (Mar. 2016), <http://myopenkimono.blogspot.com/2016/03/negligence-is-cancer-of-cyber-crime.html> (last accessed Mar. 18, 2016)

<sup>32</sup> Elizabeth Weise, *Anthem Fined \$1.7 million in 2010 breach*, (Feb. 5, 2015), <http://www.usatoday.com/story/tech/2015/02/05/anthem-health-care-computer-security-breach-fine-17-million/22931345/>.

<sup>33</sup> Ozzie Fonseca, *Following Personal Identifying Information (PII) Down the Black Net Road*, Experian (Aug. 11, 2015), <http://www.experian.com/blogs/data-breach/2015/08/11/following-personal-identifying-information-pii-down-the-black-net-road/>.

reported to view, mine and hold the hacked PII for ransom, demanding huge amounts of money from those whose PII was compromised in exchange for its return.<sup>34</sup>

69. It is telling that 21<sup>st</sup> Century Oncology offered one year of credit monitoring and identity-theft protection to 2.2 million people in its database after the FBI informed it that PII was illegally obtained by a third party in October 2015.

70. It costs 21<sup>st</sup> Century Oncology more than a *de minimis* amount to provide these services to 2.2 million data breach victims.

71. Indeed, Experian is currently charging \$4.95 a month for the first month, and then \$19.95 per month thereafter.<sup>35</sup>

72. 21<sup>st</sup> Century Oncology did so because the risk of identity theft to the Data Breach victims is not ephemeral and cannot be safely disregarded.

73. Rather, there is a strong likelihood that 21<sup>st</sup> Century Oncology victims are already or will become victims of identity fraud given the breadth of information about them that has been taken by hackers.

74. As reported by Javelin Strategy & Research's 2014 Identity Fraud Study:

Data breaches are the greatest risk factor for identity fraud. ... In 2013, one in three consumers who received notification of a data breach became a victim of fraud.<sup>36</sup>

---

<sup>34</sup> Mail Foreign Service, *Hackers demand \$10m ransom after hijacking millions of medical records*, (May 7, 2009), <http://www.dailymail.co.uk/news/article-1178276/Hackers-demand--10m-ransom-hijacking-millions-medical-records.html>.

<sup>35</sup> Experian, *Credit Monitoring*, <http://www.experian.com/consumer-products/credit-monitoring.html> (lasted visited Mar. 18, 2016).

<sup>36</sup> 2013 Identity Fraud Report: Data Breaches Becoming a Treasure Trove for Fraudsters, (Feb. 20, 2013), <https://www.javelinstrategy.com/coverage-area/2013-identity-fraud-report-data-breaches-becoming-treasure-trove-fraudsters>.

**3. The offered “remedy” is inadequate**

75. 21<sup>st</sup> Century Oncology has offered Data Breach victims twelve months of credit monitoring and identity theft insurance with ProtectMyID.com, an Experian product.

76. Neither the credit monitoring nor the insurance can prevent identity theft or fraud, even for the short twelve-month period.

**a. The offered remedies have required Data Breach victims to expend ongoing precious time containing their compromised PII**

77. Credit monitoring is reactionary and only detects activity after identity thieves use compromised PII to attempt to fraudulently open lines of credit.

78. Identity theft insurance similarly only reimburses losses after they have occurred.

79. Neither of these services prevent identity theft or fraud by: (i) detecting sales of Social Security numbers, medical information and other PII on underground black market websites before the PII is used to commit identity theft or identity fraud; (ii) monitoring public records, loan data, or criminal records; (iii) flagging existing accounts for fraud in order to thwart identity thieves’ use of compromised PII before an unauthorized transaction can be completed; or (iv) freezing credit, which prevents identity thieves’ ability to open new accounts with compromised PII.

80. Accordingly, reports have stated that 21<sup>st</sup> Century Oncology has recommended that Data Breach victims monitor their explanation of benefits statements to detect and resolve unauthorized charges without its help. As reported by *News-Press.com*:



“We also recommend that patients regularly review the explanation of benefits that they receive from their health insurer,” the letter to patients states. “If they see services that they did not receive, please contact the insurer immediately.”<sup>37</sup>

81. Also amongst the recommendations in the ProtectMyID attachment to 21<sup>st</sup> Century Oncology’s Data Breach notification letter to victims, is that they act on their own by: (a) “reviewing your credit card, bank, and other financial statements for any unauthorized activity;” (b) obtaining “a copy of your credit report ... directly from each of the three nationwide credit reporting agencies;” and (c) contacting “the Federal Trade Commission and/or the Office of the Attorney General in your home state” if Data Breach victims believe that they have become “a victim of identity theft or have reason to believe your personal information has been misused.”<sup>38</sup>

82. These tasks are significant burdens to ask of anyone who has entrusted PII to another to assume, and it is particularly despicable for 21<sup>st</sup> Century Oncology to attempt to shift its responsibility to its oncology patients and their loved ones.

**b. Thieves will likely use Data Breach victim’s PII to hurt them far longer than a year**

83. While identity thieves historically sought short-term profit from hacked credit card numbers, hackers today are targeting non-financial information so they can “continue to

---

<sup>37</sup> Frank Gluck, *Data breach affects 2.2M 21st Century Oncology patients*, News-Press.com (Mar. 10, 2016), <http://www.news-press.com/story/news/2016/03/09/data-breach-affects-22m-21st-century-oncology-patients/81525656/>.

<sup>38</sup> 21<sup>st</sup> Century, *Letter to Office of the Attorney General of New Hampshire* (March 4, 2016), <http://doj.nh.gov/consumer/security-breaches/documents/21st-century-oncology-20160304.pdf>, attached as exhibit A.

monetize victims' identifies over a longer period of time."<sup>39</sup> As observed by Gemalto vice president and CTO for data protection Jason Hart,

In 2014, consumers may have been concerned about having their credit card numbers stolen, but there are built-in protections to limit the financial risks ... However, in 2015 criminals shifted to attacks on personal information and identity theft, which are much harder to remediate once they are stolen.<sup>40</sup>

84. This truth is notably acknowledged in the ProtectMyID attachment<sup>41</sup> to 21<sup>st</sup> Century Oncology's notification letter to Data Breach victims, which states:

It is recognized that identity theft can happen months and even years after a data breach.

(i) **Compromised Social Security numbers have long-term value to thieves and long-term consequences to Data Breach victims**

85. Neal O'Farrell, a security and identity theft expert for Credit Sesame calls a Social Security number "your secret sauce," that is "as good as your DNA to hackers."<sup>42</sup>

86. Unfortunately, Data Breach victims have to wait until they become victims of Social Security number misuse before they can obtain a new one.

87. Even then, the Social Security Administration warns "that a new number probably will not solve all [] problems . . . and will not guarantee . . . a fresh start." In fact,

---

<sup>39</sup> How to Spot and Prevent Medical Identity Theft (Aug. 19, 2014), <http://www.creditcards.com/credit-card-news/spot-prevent-medical-identity-theft-1282.php>.

<sup>40</sup> Jeff Goldman, *21st Century Oncology Notifies 2.2 Million Patients of Data Breach* (Mar. 11, 2016), <http://www.esecurityplanet.com/network-security/21st-century-oncology-notifies-2.2-million-patients-of-data-breach.html>.

<sup>41</sup> 21<sup>st</sup> Century, *Letter to Office of the Attorney General of New Hampshire* (March 4, 2016), <http://doj.nh.gov/consumer/security-breaches/documents/21st-century-oncology-20160304.pdf>, attached as exhibit A.

<sup>42</sup> How to Protect Your Kids From the Anthem Data Breach, (Feb. 10, 2015), <http://www.kiplinger.com/article/credit/T048-C011-S001-how-to-protect-your-kids-from-the-anthem-data-brea.html#>.

“[f]or some victims of identity theft, a new number actually creates new problems.”<sup>43</sup> One of those new problems is that a new Social Security number will have a completely blank credit history, making it difficult to get credit for years unless it is linked to the old compromised number.

**(ii) Compromised medical information has even greater long-term value to thieves and consequences to Data Breach victims**

88. Kunal Rupani, director of product management at Accellion, told *eSecurity Planet* that it’s likely the 21<sup>st</sup> Century Oncology hackers were targeting the Data Breach victims’ healthcare data for its long-term value, stating:

“Unlike credit card numbers and other financial data, healthcare information doesn’t have an expiration date,” he said. “As a result, a patient’s records can sell on the black market for upwards of fifty times the amount of their credit card number, making hospitals and other healthcare organizations extremely lucrative targets for cybercriminals.”<sup>44</sup>

89. According to a study by Dell SecureWorks, when such medical information is “packaged with other PII can net a seller more than \$1,000 for each package.”<sup>45</sup>

---

<sup>43</sup> Identity Theft and Your Social Security Number, <https://www.ssa.gov/pubs/EN-05-10064.pdf> at pgs. 6-7 (last accessed Mar. 18, 2016).

<sup>44</sup> Jeff Goldman, *21st Century Oncology Notifies 2.2 Million Patients of Data Breach* (Mar. 11, 2016), <http://www.csecurityplanet.com/network-security/21st-century-oncology-notifies-2.2-million-patients-of-data-breach.html>.

<sup>45</sup> Following Personal Identifying Information (PII) Down the Black Net Road, (Aug. 11, 2015), <http://www.experian.com/blogs/data-breach/2015/08/11/following-personal-identifying-information-pii-down-the-black-net-road/>.

90. Once hackers have a medical ID, they can use it to procure prescription drugs, expensive medical equipment, or simply to commit financial fraud—often for months or years before the Data Breach victim or anyone else notices.”<sup>46</sup>

91. After use of compromised non-financial PII is detected, the emotional and economic consequences to the Data Breach victim are significant. As reported by CreditCards.com:

The Ponemon Institute found that 36 percent of medical ID theft victims pay to resolve the issue, and their out-of-pocket costs average nearly \$19,000. Even if you don’t end up paying out of pocket, such usage can wreak havoc on both medical and credit records, and clearing that up is a time-consuming headache. That’s because medical records are scattered. Unlike personal financial information, which is consolidated and protected by credit bureaus, bits of your medical records end up in every doctor’s office and hospital you check into, every pharmacy that fills a prescription and every facility that processes payments for those transactions.<sup>47</sup>

92. Furthermore, the Office of Inspector General of the U.S. Department of Health & Human Services has cautioned that the consequences to Data Breach victims can be medically disastrous:

The damage can be life-threatening to you if the wrong information ends up in your personal medical records.<sup>48</sup>

**4. The delayed disclosure further harmed Data Breach victims**

93. In the intervening months between when the FBI notified 21<sup>st</sup> Century Oncology of the Data Breach and when 21<sup>st</sup> Century Oncology finally disclosed the Data Breach to its patients, 21<sup>st</sup> Century Oncology focused *not* on protecting patients and others

---

<sup>46</sup> How to Spot and Prevent Medical Identity Theft (Aug. 19, 2014), <http://www.creditcards.com/credit-card-news/spot-prevent-medical-identity-theft-1282.php>.

<sup>47</sup> *Id.*

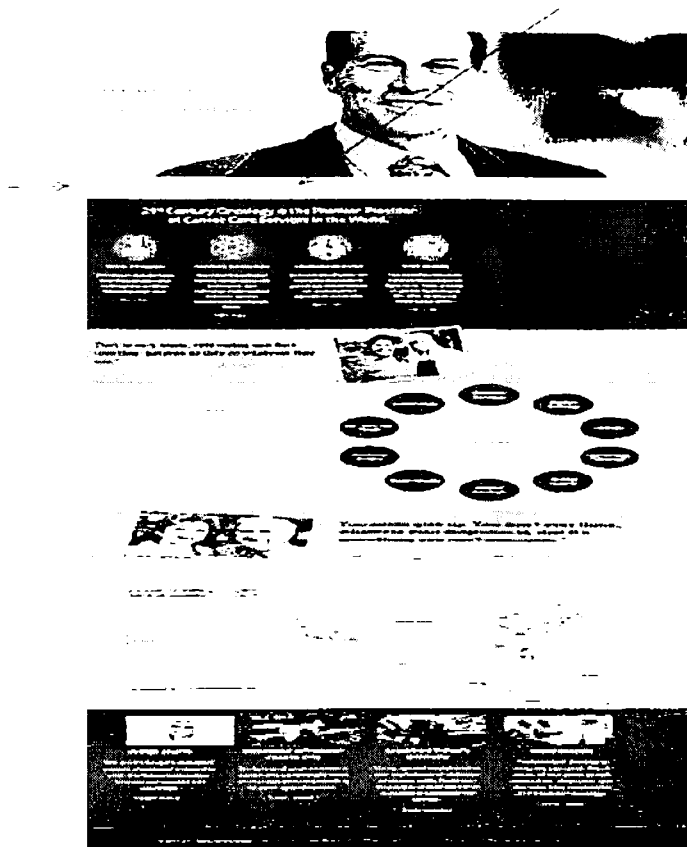
<sup>48</sup> Medical ID Theft/Fraud Information, <http://oig.hhs.gov/fraud/medical-id-theft/> (last accessed Mar. 18, 2016).

whose PII it had collected and retained, but rather on controlling the damage to itself and its investors.

94. On information and belief, despite having months to prepare notification letters for the Data Breach victims after being notified of it by the FBI, 21<sup>st</sup> Century Oncology waited a week after announcing the Data Breach to its investors on March 4, 2016 to mail notification letters to Data Breach victims.

95. When Data Breach victims began receiving the notification letters from 21<sup>st</sup> Century Oncology on or about March 12, 2016, some of them did not understand that they had a relationship with 21<sup>st</sup> Century Oncology and believed the notification letters themselves to be a scam.

96. Indeed, as of March 18, 2016, it is not obvious to a Data Breach victim looking to confirm the authenticity of the notification letter through 21<sup>st</sup> Century Oncology's website that there has been a data breach. While a single line, "A Message to Our Patients Regarding Security Incident" appears on the home page of 21<sup>st</sup> Century Oncology's website, it does not prominently appear at the top or bottom of the screen, and is masked amongst other text and images on the elongated home page that requires one to scroll to reach the bottom:



97. Other Data Breach victims who were unfamiliar with the name “21<sup>st</sup> Century Oncology” were left to play detective to ascertain which of their current or past treating physicians were associated with 21<sup>st</sup> Century Oncology.

98. In addition, the notification letters that 21<sup>st</sup> Century Oncology ultimately mailed to Data Breach victims failed to provide concrete information about the Data Breach, and incompletely described what PII was in fact exposed, how it was exposed, and what changes 21<sup>st</sup> Century Oncology was making to prevent further compromises of PII in the future.

99. Making matters worse, Data Breach victims have felt blindsided by the notification that their Social Security numbers were accessed with only weeks remaining before the tax filing deadline and have found activating the credit monitoring service to be

confusing and time consuming, thereby increasing their anxiety that the Data Breach would potentially jeopardize any expected tax refund.

100. Accordingly, 21<sup>st</sup> Century Oncology's delayed and insufficient response to the Data Breach created additional hardships for these Data Breach victims during an already medical and financial stressful time.

**F. 21<sup>st</sup> Century Oncology's Priorities Have Caused Plaintiffs' Most Sensitive PII to Be Compromised, Increasing Their Current and Ongoing Suffering**

**1. Plaintiff Veneta Delucchi**

101. On or about March 18, 2016, Plaintiff Veneta Delucchi received a notice from 21<sup>st</sup> Century Oncology informing her that the FBI advised 21<sup>st</sup> Century Oncology that patient information was illegally obtained by an unauthorized third party.

102. Data that may have been obtained include her name, Social Security number, physician's name, diagnosis and treatment information, and insurance information.

103. Plaintiff was disturbed and disappointed that 21<sup>st</sup> Century Oncology did not protect her private and sensitive medical and other PII and, on or about March 18, 2016, signed up for a one-year membership of Experian's ProtectMyID Alert.

104. Plaintiff anticipates spending considerable time and money indefinitely to contain the impact of 21<sup>st</sup> Century Oncology's Data Breach on Plaintiff's compromised PII and believes one year of credit monitoring offered by 21<sup>st</sup> Century Oncology through a single credit reporting agency, without any type of monitoring of medical or tax records, to be insufficient.

**2. Plaintiff Bradley Bernius**

105. Although Plaintiff Bradley Bernius received treatment from 21<sup>st</sup> Century Oncology in its Redding, California facility from March 2011 through approximately March 2012, to date, he has not received a letter notifying him of the Data Breach. Nonetheless, he reasonably believes he is one of the approximately 2.2 million victims of the Data Breach because he provided his medical information and other PII 21<sup>st</sup> Century Oncology since March 2011. Additionally, when he and his caretaker called 21<sup>st</sup> Century Oncology in April 2016, 21<sup>st</sup> Century Oncology confirmed that Plaintiff Bernius' PII was contained in the database compromised in the Data Breach.

106. Data that may have been obtained include his name, Social Security number, physician's name, diagnosis and treatment information, and insurance information.

107. Plaintiff Bernius is experiencing stress and anxiety as a result of the Data Breach because in addition to his caring for his medical condition, he has had to spend numerous hours investigating the Data Breach, enrolling in credit monitoring service, and reviewing his credit reports and financial statements for fraudulent activity. In addition, Plaintiff Bernius anticipates spending considerable time and money indefinitely to contain the impact of 21<sup>st</sup> Century Oncology's Data Breach on his compromised PII.

**VI. CLASS ACTION ALLEGATIONS**

108. Plaintiffs bring claims pursuant to Federal Rule of Civil Procedure 23 on behalf of a Class of similarly situated persons, which Plaintiffs initially propose to be defined as follows:

All persons in the United States whose PII was compromised as a result of the Data Breach.



109. In addition, Plaintiffs brings claim pursuant to Federal Rule of Civil Procedure 23 on behalf of a Subclass of similarly situated persons, which Plaintiffs initially propose to be defined as follows:

All persons in California whose PII was compromised as a result of the Data Breach.

110. **Numerosity.** The proposed Class is sufficiently numerous, as 2.2 million Data Breach victims have had their PII compromised and they are dispersed throughout the United States, making joinder of all members impracticable. Class members can be readily identified by records maintained by 21<sup>st</sup> Century Oncology.

111. **Commonality.** Common questions of fact and law exist for each cause of action and predominate over questions affecting only individual class members, including:

- a. Whether 21<sup>st</sup> Century Oncology had a legal duty to use reasonable security measures to protect Class members' PII;
- b. Whether 21<sup>st</sup> Century Oncology timely, accurately, and adequately informed Class members that their PII had been compromised;
- c. Whether 21<sup>st</sup> Century Oncology breached its legal duty by failing to protect Class members' PII;
- d. Whether 21<sup>st</sup> Century Oncology acted reasonably in securing Class members' PII;
- e. Whether Class members are entitled to actual damages and/or statutory damages; and
- f. Whether Class members are entitled to injunctive relief.

112. **Typicality.** Plaintiffs' claims are typical of the claims of members of the proposed Class because, among other things, Plaintiffs and Class members sustained similar injuries as a result of 21<sup>st</sup> Century Oncology's uniform wrongful conduct and their legal claims all arise from the same conduct by 21<sup>st</sup> Century Oncology.

113. **Adequacy.** Plaintiffs will fairly and adequately protect the interests of the proposed Class. Plaintiffs' interests do not conflict with Class members' interests and they have retained counsel experienced in complex class action and data privacy litigation to prosecute this case on behalf of the Class.

114. **Rule 23(b)(3).** In addition to satisfying the prerequisites of Rule 23(a), Plaintiffs satisfy the requirements for maintaining a class action under Rule 23(b)(3). Common questions of law and fact predominate over any questions affecting only individual class members and a class action is superior to individual litigation. The amount of damages available to individual plaintiffs is insufficient to make litigation addressing 21<sup>st</sup> Century Oncology's conduct economically feasible in the absence of the class action procedure. Individualized litigation also presents a potential for inconsistent or contradictory judgments, and increases the delay and expense to all parties and the court system presented by the legal and factual issues of the case. By contrast, the class action device presents far fewer management difficulties and provides the benefits of a single adjudication, economy of scale, and comprehensive supervision by a single court.

115. **Rule 23(b)(2).** Plaintiffs also satisfy the requirements for maintaining a class action under Rule 23(b)(2). 21<sup>st</sup> Century Oncology has acted or refused to act on grounds that

apply generally to the proposed Class, making final declaratory or injunctive relief appropriate with respect to the proposed Class as a whole.

116. **Rule 23(c)(4).** This action also satisfies the requirements for maintaining a class action under Rule 23(c)(4). The claims of Class members are composed of particular issues that are common to all Class members and capable of class wide resolution that will significantly advance the litigation.

## **VII. CAUSES OF ACTION**

### **COUNT I Negligence**

117. Plaintiffs reallege and incorporate by reference the allegations contained in each of the preceding paragraphs as if fully set forth herein.

118. In collecting and retaining the medical and other PII of patients and other Data Breach victims, 21<sup>st</sup> Century Oncology owed Plaintiffs and Class members a duty to exercise reasonable care in safeguarding and protecting that information. This duty included, among other things, maintaining and testing 21<sup>st</sup> Century Oncology's security systems and taking other reasonable security measures to protect and adequately secure the PII of Plaintiffs and class members from unauthorized access.

119. 21<sup>st</sup> Century Oncology's security system and procedures for handling the medical and other PII of victims were intended to and did affect Plaintiffs and Class members. 21<sup>st</sup> Century Oncology knew that by collecting and storing victims' private and sensitive medical and other PII, it undertook a responsibility to take reasonable security measures to protect the information from being stolen and exposed to unauthorized persons.

120. 21<sup>st</sup> Century Oncology owed a duty of care to Plaintiffs and Class members because they were foreseeable and probable victims of any inadequate security practices. It was foreseeable that if 21<sup>st</sup> Century Oncology did not take reasonable security measures, the PII of Plaintiffs and members of the Class would be stolen. Major corporations like 21<sup>st</sup> Century Oncology face a higher threat of security breaches than smaller companies due in part to the large amounts of data they possess. 21<sup>st</sup> Century Oncology knew or should have known its security systems were inadequate, particularly in light of the prior data breach that 21<sup>st</sup> Century Oncology experienced, and yet 21<sup>st</sup> Century Oncology failed to take reasonable precautions to safeguard the PII of patients and other Data Breach victims.

121. The duty 21<sup>st</sup> Century Oncology owed to Plaintiffs and members of the Class to protect their PII is also underscored by Fla. Stat. § 501.171(2), the Health Insurance Portability and Accountability Act (“HIPAA”), 42 U.S.C. § 1320d *et seq.*, and the Health Information Technology Act (“HITECH Act”), 42 U.S.C. § 17901, *et seq.*, which recognize the importance of maintaining the confidentiality of personal and medical information and were enacted to protect individuals from the unauthorized exposure of their personal and medical information.

122. 21<sup>st</sup> Century Oncology also had a duty to timely disclose to Plaintiffs and Class members that their PII had been or was reasonably believed to have been compromised. Timely disclosure was necessary so that Plaintiffs and members of the Class could, among other things: (i) buy identity protection, monitoring, and recovery services; (ii) flag asset, credit, and tax accounts for fraud, including reporting the theft of their Social Security numbers to financial institutions, credit agencies, and the Internal Revenue Service; (iii) purchase or

otherwise obtain credit reports; (iv) monitor credit, financial, utility, explanation of benefits, and other account statements on a monthly basis for unrecognized credit inquiries, Social Security numbers, home addresses, charges, and/or medical services; (v) place and renew credit fraud alerts on a quarterly basis; (vi) routinely monitor public records, loan data, or criminal records; (vii) contest fraudulent charges and other forms of criminal, financial and medical identity theft, and repair damage to credit and other financial accounts; and (viii) take other steps to protect themselves and recover from identity theft and fraud.

123. As a result of 21<sup>st</sup> Century Oncology's negligence, Plaintiffs and members of the Class have suffered and will suffer injury, including but not necessarily limited to: (1) the loss of the opportunity to control how their PII is used; (2) the diminution in the value and/or use of their PII; (3) the compromise, publication, and/or theft of their PII; (4) out-of-pocket costs associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of medical accounts; (5) lost opportunity costs associated with effort expended and the loss of productivity from addressing and attempting to mitigate the actual and future consequences of the breach, including but not limited to efforts spent researching how to prevent, detect, contest and recover from identity and health care/medical data misuse; (6) costs associated with the inability to use credit and assets frozen or flagged due to credit misuse, including complete credit denial and/or increased costs to use credit, credit scores, credit reports and assets; (7) unauthorized use of compromised PII to open new financial and/or health care or medical accounts; (8) tax fraud and/or other unauthorized charges to financial, health care or medical accounts and associated lack of access to funds while proper information is confirmed and corrected; (9) the continued risk to their PII, which remains in 21<sup>st</sup> Century

Oncology's possession and is subject to further breaches so long as 21<sup>st</sup> Century Oncology fails to undertake appropriate and adequate measures to protect the PII in its possession; and (10) future costs in terms of time, effort and money that will be expended, to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of the Class members.

124. As a result of 21<sup>st</sup> Century Oncology's negligence, Plaintiffs and members of the Class have suffered and will suffer injury, including but not necessarily limited to: (1) anxiety, stress and emotional distress; (2) the loss of the opportunity to control how their PII is used; (3) the diminution in the value and/or use of PII entrusted to 21<sup>st</sup> Century Oncology for the purpose of deriving medical care, when Plaintiffs and Class members understood that their PII would be safeguarded against unauthorized use; and (4) the compromise, disclosure and/or sale of their PII.

125. There is a very close connection between 21<sup>st</sup> Century Oncology's failure to employ reasonable security protections of patient and other Data Breach victims' PII and the injuries suffered by Plaintiffs and Class members. When individuals have their PII stolen, they are at risk for identity theft, and need to: (i) buy identity protection, monitoring, and recovery services; (ii) flag asset, credit, and tax accounts for fraud, including reporting the theft of their Social Security numbers to financial institutions, credit agencies, and the Internal Revenue Service; (iii) purchase or otherwise obtain credit reports; (iv) monitor credit, financial, utility, explanation of benefits, and other account statements on a monthly basis for unrecognized credit inquiries, Social Security numbers, home addresses, charges, and/or medical services; (v) place and renew credit fraud alerts on a quarterly basis; (vi) routinely monitor public

records, loan data, or criminal records; (vii) contest fraudulent charges and other forms of criminal, financial and medical identity theft, and repair damage to credit and other financial accounts; and (viii) take other steps to protect themselves and recover from identity theft and fraud.

126. 21<sup>st</sup> Century Oncology is responsible for not protecting the PII of its patients and other Data Breach victims. If 21<sup>st</sup> Century Oncology had reasonable security measures in place, data thieves would not have been able to steal and expose the PII of millions of patients and other Data Breach victims.

127. The policy of preventing future harm weighs strongly in favor of finding a special relationship between 21<sup>st</sup> Century Oncology and its patients and other Data Breach victims. Patients and other Data Breach victims were required to share private and sensitive medical and/or other PII with 21<sup>st</sup> Century Oncology as a condition of receiving medical care and depended on 21<sup>st</sup> Century Oncology as a medical provider to ensure that this information was protected from theft and unauthorized disclosure. If companies are not held accountable for failing to take reasonable security measures to protect this PII, they will not take the steps that are necessary to protect against future data breaches.

128. 21<sup>st</sup> Century Oncology breached its duty to exercise reasonable care in protecting the PII of Plaintiffs and the Class by failing to implement and maintain adequate security measures to safeguard this PII, failing to monitor its systems to identify suspicious activity, and allowing unauthorized access to the PII of Plaintiffs and Class members.

129. 21<sup>st</sup> Century Oncology breached its duty to timely notify Plaintiffs and the Class about the Data Breach. 21<sup>st</sup> Century Oncology waited months after discovering the Data

Breach, and five months after the actual breach, to inform victims that their PII had been or was reasonably believed to have been compromised.

130. But for 21<sup>st</sup> Century Oncology's failure to implement and maintain adequate security measures to protect victims' PII and failure to monitor its systems to identify suspicious activity, the PII of Plaintiffs and Class members would not have been compromised, Plaintiffs and Class members would not have been injured, and Plaintiffs and Class members would not be at a heightened risk of identity theft in the future.

131. 21<sup>st</sup> Century Oncology's negligence was a substantial factor in causing harm to Plaintiffs and Class members. As a direct and proximate result of 21<sup>st</sup> Century Oncology's failure to exercise reasonable care and use commercially reasonable security measures, the PII of patients and other Data Breach victims was accessed by unauthorized individuals who can continue to use this compromised PII to commit identity theft and identity and health care and/or medical fraud indefinitely.

132. As a result of 21<sup>st</sup> Century Oncology's negligence, Plaintiffs and the Class members suffered and will continue to suffer injury and/or harm including, but not limited to anxiety, stress, emotional distress, loss of privacy, loss of control over their PII, and other economic and non-economic losses.

133. As a result of 21<sup>st</sup> Century Oncology's negligence, Plaintiffs and members of the Class are entitled to injunctive relief, including, but not limited to an order that 21<sup>st</sup> Century Oncology: (1) engage third party security auditors/penetration testers as well as internal security personnel to conduct testing consistent with prudent industry practices, including simulated attacks, penetration tests, and audits on 21<sup>st</sup> Century Oncology's systems on a



periodic basis; (2) engage third party security auditors and internal personnel to run automated security monitoring consistent with prudent industry practices; (3) audit, test, and train its security personnel regarding any new or modified procedures; (4) purge, delete and destroy, in a secure manner, PII not necessary for its business operations; (5) conduct regular database scanning and securing checks consistent with prudent industry practices; (6) periodically conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach consistent with prudent industry practices; (7) receive periodic compliance audits by a third party regarding the security of the computer systems 21<sup>st</sup> Century Oncology uses to store PII; (8) meaningfully educate patients and other Data Breach victims about the threats they face as a result of the loss of their PII to third parties, as well as the steps they must take to protect themselves; and (9) provide ongoing identity theft protection, monitoring, and recovery services to Plaintiffs and Class members.

134. Plaintiffs and the Class are also entitled to damages and reasonable attorneys' fees and costs. Plaintiffs also seek reasonable attorneys' fees and costs under applicable law including Federal Rule of Civil Procedure 23.

**COUNT II**  
**Breach of Implied Covenant of Good Faith and Fair Dealing**

135. Plaintiffs reallege and incorporate by reference the allegations contained in each of the preceding paragraphs as if fully set forth herein.

136. Plaintiffs and Class Members entered into and/or were the beneficiaries of contracts with 21<sup>st</sup> Century Oncology.

137. These contracts were subject to implied covenants of good faith and fair dealing that all parties would act in good faith and with reasonable efforts to perform their contractual obligations (both explicit and fairly implied) and would not impair the rights of the other parties to receive their rights, benefits, and reasonable expectations under the contracts. These included the covenants that 21<sup>st</sup> Century Oncology would act fairly, reasonably, and in good faith in carrying out their contractual obligations to protect the confidentiality of Plaintiffs' and Class members' PII and to comply with industry standards and federal and state laws and regulations for the security of this information.

138. Plaintiffs and Class members who obtained and/or paid for medical care entrusted their sensitive PII to 21<sup>st</sup> Century Oncology.

139. 21<sup>st</sup> Century Oncology promised to take specific measures to protect Plaintiffs' and Class members' PII. 21<sup>st</sup> Century Oncology breached the covenant of good faith and fair dealing by failing to take adequate measures to protect the confidentiality of Plaintiffs' and Class Members' PII, resulting in the Data Breach. 21<sup>st</sup> Century Oncology unreasonably interfered with the contract benefits owed to Plaintiffs and Class members by: compiling and storing Plaintiffs' and Class members' data in one massive database; failing to implement reasonable and adequate security measures to protect and limit access to the PII in the database; and failing to implement reasonable auditing procedures to detect and halt the unauthorized extraction of data.

140. Plaintiffs and Class members performed all conditions, covenants, obligations, and promises owed to 21<sup>st</sup> Century Oncology, including paying for the medical care associated

with 21<sup>st</sup> Century Oncology and/or providing 21<sup>st</sup> Century Oncology the confidential information required by the contracts.

141. As a result of 21<sup>st</sup> Century Oncology's breach of the implied covenant, Plaintiffs and Class members did not receive the full benefit of their bargain, and instead received medical care that was less valuable than what they paid for and less valuable than their reasonable expectations under the contracts. Plaintiffs and Class members were damaged in an amount at least equal to the difference in value between that which they reasonably expected under the contracts and 21<sup>st</sup> Century Oncology's partial, deficient and/or defective performance.

142. In addition, as a result of 21<sup>st</sup> Century Oncology's breach of the covenant of good faith and fair dealing, Plaintiffs and Class members have suffered actual damages resulting from their attempt to ameliorate the effect of the Data Breach and remain at imminent risk of suffering additional damages in the future.

143. Accordingly, Plaintiffs and Class members have been injured as a result of 21<sup>st</sup> Century Oncology's breaches of the covenant of good faith and fair dealing and are entitled to damages and/or restitution in an amount to be proven at trial.

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

144. Plaintiffs reallege and incorporate by reference the allegations contained in each of the preceding paragraphs as if fully set forth herein.

145. The Florida Deceptive and Unfair Trade Practices Act ("FDUTPA") was enacted 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).

146. Plaintiffs and the Class are “consumers” as defined by Florida Statute § 501.203(7), and the subject transactions are “trade or commerce” as defined by Florida Statute § 501.203(8).

147. 21<sup>st</sup> Century Oncology violated and continues to violate the FDUTPA by engaging in the described unconscionable, deceptive, unfair acts or practices proscribed by Florida Statute § 501.201, *et seq.*, including, but not limited to breaching its duty pursuant to Fla. Stat. § 501.171(2), to Plaintiffs and Class members to implement and maintain reasonable security procedures and practices to safeguard Plaintiffs’ and Class members’ PII by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiffs’ and Class members’ PII.

148. Had Plaintiffs and Class members known of 21<sup>st</sup> Century Oncology’s inability to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiffs’ and class members’ PII they would not have obtained care through providers employed by or affiliated with 21<sup>st</sup> Century Oncology.

149. By omitting the fact that 21<sup>st</sup> Century Oncology could not provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiffs’ and class members’ PII, 21<sup>st</sup> Century Oncology violated the FDUTPA.

150. Plaintiffs and the Class reasonably relied upon 21<sup>st</sup> Century Oncology’s omissions in obtaining and/or paying for medical care from providers employed by or affiliated with 21<sup>st</sup> Century Oncology.

151. 21<sup>st</sup> Century Oncology's omissions regarding its ability to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiffs' and Class members' PII was an act likely to mislead Plaintiffs and the members of the Class acting reasonably under the circumstances, and constitutes an unfair and deceptive trade practice in violation of the FDUTPA.

152. 21<sup>st</sup> Century Oncology knew or should have known that it had kept highly relevant and material information—namely, information regarding its inability to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiffs' and class members' PII—from its patients, and therefore violated the FDUTPA.

153. As a direct and proximate result of 21<sup>st</sup> Century Oncology's violation of the FDUTPA, Plaintiffs and Class members have suffered harm in the form of monies paid to 21<sup>st</sup> Century Oncology.

154. Plaintiffs and the Class also seek equitable relief and to enjoin 21<sup>st</sup> Century Oncology on the terms that the Court considers reasonable.

155. In addition, Plaintiffs and the Class seek reasonable attorneys' fees and costs incurred in bringing this action.

**COUNT IV**  
**Violation of the California Confidentiality of Medical Information Act**  
**Cal. Civ. Code § 56, *et seq.***  
**(On behalf of the California Subclass)**

156. Plaintiffs reallege and incorporate by reference the allegations contained in each of the preceding paragraphs as if fully set forth herein.

157. Plaintiffs bring this cause of action on behalf of the California Subclass.

158. California's Confidentiality of Medical Information Act ("CMIA") requires a healthcare provider "who creates, maintains, preserves, stores, abandons, destroys, or disposes of medical information [to] do so in a manner that preserves the confidentiality of the information contained therein. Any provider of health care, health care service plan, pharmaceutical company, or contractor who negligently creates, maintains, preserves, stores, abandons, destroys, or disposes of medical information shall be subject to the remedies and penalties provided under subdivisions (b) and (c) of Section 56.36." Cal. Civ. Code § 56.101. The CMIA requires that "[a]n electronic health record system or electronic medical record system . . . [p]rotect and preserve the integrity of electronic medical information." Cal. Civ. Code section 56.101(b).

159. 21<sup>st</sup> Century Oncology is a "provider of health care" "who creates, maintains, preserves, stores, abandons, destroys, or disposes of medical information" pursuant to Cal. Civ. Code sections 56.05(m) and 56.101.

160. The PII compromised in the Data Breach constitutes or includes "medical information" maintained in electronic form pursuant to Cal. Civ. Code section 56.05(j).

161. 21<sup>st</sup> Century Oncology has violated section the CMIA by negligently maintaining, preserving and storing the PII of Plaintiffs and members of the California Subclass, and by failing to protect and preserve the integrity of the PII of Plaintiffs and members of the California Subclass .

162. 21<sup>st</sup> Century Oncology failed to obtain written authorization from Plaintiffs and members of the California Subclass to disclose or release their medical information, which must meet the following requirements pursuant to Cal. Civ. Code section 56.11:

- a. The authorization must be handwritten by the patient who signs it or in typeface no smaller than 14-point font;
- b. The authorization must be clearly separate from any other language on the same page and must be executed by a signature that serves no purpose other than to execute the authorization;
- c. The authorization must be signed by the patient, the patient's legal representative, or the patient's spouse;
- d. The authorization must specify the uses and limitations on the types of medical information to be disclosed;
- e. The authorization must state the name or functions of the provider of health care, health care service plan, pharmaceutical company, or contractor that may disclose the medical information, the name or functions of the persons or entities authorized to receive the medical information, and the specific uses and limitations of the medical information by the persons or entities authorized to receive the medical information;
- f. The authorization must specify the date after which the provider of health care, health care service plan, pharmaceutical company, or contractor is no longer authorized to disclose the medical information; and
- g. The authorization must advise the person signing the authorization of the right to receive a copy of the authorization.

163. As a result of the Data Breach, PII of Plaintiffs and members of the California Subclass has been compromised and accessed without authorization by third parties. Among

other things, 21<sup>st</sup> Century Oncology is and was negligent in failing to use reasonable security procedures to prevent unauthorized access to files containing the PII; failing to use reasonable authentication procedures so that PII could be tracked in case of a security breach; failing to timely detect that PII was compromised in the Data Breach; and allowing undetected and unauthorized access where PII was kept, all in violation of the CMLA, HIPAA, and the HITECH Act.

164. 21<sup>st</sup> Century Oncology's failure to implement adequate security measures to protect the PII of Plaintiffs and members of the California Subclass was a substantial factor in allowing hackers to breach its computer systems and access the PII.

165. As a direct and proximate result of 21<sup>st</sup> Century Oncology's violations of the CMLA, 21<sup>st</sup> Century Oncology has allowed Plaintiffs' and the Subclass's PII to: (a) escape and spread from its normal place of storage through unauthorized disclosure or release; and (b) be accessed by an unauthorized third person or persons and illegally obtained, on information and belief, in order to view, mine, exploit, use and/or profit from it, thereby breaching the confidentiality of their PII. Plaintiffs and the California Subclass have accordingly sustained and will continue to sustain actual damages as set forth above.

166. Plaintiffs, individually and on behalf of members of the California Subclass, seek actual and statutory damages pursuant to Cal. Civ. Code section 56.36(b) and (c), and an injunction requiring 21<sup>st</sup> Century Oncology to formulate, adopt, and implement a data security plan that prevents unauthorized access to PII.

167. Plaintiffs also seek reasonable attorneys' fees and costs under applicable law including Federal Rule of Civil Procedure 23 and California Code of Civil Procedure § 1021.5.



**COUNT V**  
**Violations of the Customer Records Act**  
**Cal. Civ. Code § 1798.81.5, *et seq.***  
**(On behalf of the California Subclass)**

168. Plaintiffs reallege and incorporate by reference the allegations contained in each of the preceding paragraphs as if fully set forth herein.

169. Plaintiffs bring this cause of action on behalf of the California Subclass.

170. The California Legislature enacted Cal. Civ. Code section 1798.81.5 “to ensure that personal information about California residents is protected.” The statute requires that any business that “owns, licenses, or maintains personal information about a California resident . . . implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure.”<sup>21</sup> Century Oncology is a “business” as defined by Cal. Civ. Code section 1798.80(a).

171. Plaintiffs and members of the California Subclass are each an “individual” as defined by Cal. Civil Code section 1798.80(d).

172. The PII compromised in the Data Breach constitutes “personal information” as defined by Cal. Civil Code sections 1798.80(e) and 1798.81.5(d), which includes “information that identifies, relates to, describes, or is capable of being associated with, a particular individual, including, but not limited to, his or her name, signature, Social Security number, physical characteristics or description, address, telephone number, passport number, driver’s license or state identification card number, insurance policy number, education, employment, employment history, bank account number, credit card number, debit card number, or any other financial information, medical information, or health insurance information.”

173. By failing to implement reasonable security measures appropriate to the nature of the personal information of its current and former employees, 21<sup>st</sup> Century Oncology violated Cal. Civ. Code section 1798.81.5.

174. As a result of 21<sup>st</sup> Century Oncology's violation of Cal. Civil Code section 1798.81.5, Plaintiffs and members of the California Subclass have sustained and will continue to sustain actual damages as set forth above.

175. Plaintiffs seek all remedies available under Cal. Civil Code section 1798.84, including actual and statutory damages, equitable relief, and reasonable attorneys' fees. Plaintiffs also seek reasonable attorneys' fees and costs under applicable law including Federal Rule of Civil Procedure 23 and California Code of Civil Procedure § 1021.5.

176. Due to its violation of Cal. Civil Code section 1798.81.5, 21<sup>st</sup> Century Oncology "may be enjoined" under Cal. Civil Code section 1798.84(e). Accordingly, Plaintiffs seek an injunction requiring 21<sup>st</sup> Century Oncology to formulate, adopt, and implement a data security plan that prevents unauthorized access to PII.

**COUNT VI**  
**Declaratory Judgment**

177. Plaintiffs reallege and incorporate by reference the allegations contained in each of the preceding paragraphs as if fully set forth herein.

178. As previously alleged, Plaintiffs and the Class have stated claims against 21<sup>st</sup> Century Oncology based on negligence, implied covenant of good faith and fair dealing, and violations of the FDUTPA, CMIA, and CRA.

179. 21<sup>st</sup> Century Oncology has failed to live up to its obligations to provide reasonable security measures for the PII of Plaintiffs and the Class, as indicated by its corporate history of security breaches and the specific Data Breach that precipitated this lawsuit.

180. In addition, the Data Breach has rendered 21<sup>st</sup> Century Oncology's system even more vulnerable to unauthorized access and requires that 21<sup>st</sup> Century Oncology immediately take even more stringent measures to currently safeguard the PII of Plaintiffs and the Class going forward.

181. An actual controversy has arisen in the wake of 21<sup>st</sup> Century Oncology's Data Breach regarding 21<sup>st</sup> Century Oncology's *current* obligations to provide reasonable data security measures to protect the PII of Plaintiffs and the Class. On information and belief, 21<sup>st</sup> Century Oncology maintains that its security measures were, and remain, reasonably adequate. On information and belief, 21<sup>st</sup> Century Oncology further denies that it previously had or now has any obligation to better safeguard the PII of Plaintiffs and the Class.

182. Plaintiffs thus seek a declaration that to comply with its existing obligations, 21<sup>st</sup> Century Oncology must implement specific additional, prudent industry security practices, as outlined below, to provide reasonable protection and security to the PII of Plaintiffs and the Class.

183. Specifically, Plaintiffs and the Class seek a declaration that 21<sup>st</sup> Century Oncology's existing security measures do not comply with its obligations, and that to comply with its obligations, 21<sup>st</sup> Century Oncology must implement and maintain reasonable security measures on behalf of Plaintiffs and the Class, including, but not limited to: (1) engaging third party security auditors/penetration testers as well as internal security personnel to conduct

testing consistent with prudent industry practices, including simulated attacks, penetration tests, and audits on 21<sup>st</sup> Century Oncology's systems on a periodic basis; (2) engaging third party security auditors and internal personnel to run automated security monitoring consistent with prudent industry practices; (3) auditing, testing, and training its security personnel regarding any new or modified procedures; (4) purging, deleting and destroying, in a secure manner, PII not necessary for its business operations; (5) conducting regular database scanning and securing checks consistent with prudent industry practices; (6) periodically conducting internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach consistent with prudent industry practices; (7) receiving periodic compliance audits by a third party regarding the security of the computer systems 21<sup>st</sup> Century Oncology uses to store PII; (8) meaningfully educating patients and other Data Breach victims about the threats they face as a result of the loss of their PII to third parties, as well as the steps they must take to protect themselves; and (9) providing ongoing identity theft protection, monitoring, and recovery services to Plaintiffs and class members, as well as their dependents and designated beneficiaries of employment-related benefits through 21<sup>st</sup> Century Oncology.

**COUNT VII**  
**Unjust Enrichment**

184. In the alternative, Plaintiffs allege that Plaintiffs and the Class have no adequate remedy at law.

185. Plaintiffs and Class members conferred a monetary benefit on 21<sup>st</sup> Century Oncology in the form of money paid (directly or indirectly) to 21<sup>st</sup> Century Oncology for medical services obtained and/or provided their PII to 21<sup>st</sup> Century Oncology.

186. 21<sup>st</sup> Century Oncology appreciated or had knowledge of the benefits conferred upon it by Plaintiffs and Class members.

187. The money that Plaintiffs and Class members paid (directly or indirectly) to 21<sup>st</sup> Century Oncology should have been used by 21<sup>st</sup> Century Oncology, in part, to pay for the administrative costs of reasonable data privacy and security practices and procedures.

188. As a result of 21<sup>st</sup> Century Oncology's conduct, Plaintiffs and Class members suffered actual damages in an amount equal to the difference in value between the medical care with the reasonable data privacy and security practices and procedures that Plaintiffs and Class members paid for, and the medical care without reasonable data privacy and security practices and procedures that they received.

189. Under principles of equity and good conscience, 21<sup>st</sup> Century Oncology should not be permitted to retain the money belonging to Plaintiffs and Class members because 21<sup>st</sup> Century Oncology failed to implement (or adequately implement) the data privacy and security practices and procedures that Plaintiffs and Class members paid for and that were otherwise mandated by HIPAA and HITECH Act regulations, federal, state and local laws, and industry standards.

190. 21<sup>st</sup> Century Oncology should be compelled to disgorge into a common fund for the benefit of Plaintiffs and Class members all unlawful or inequitable proceeds received by 21<sup>st</sup> Century Oncology.

191. A constructive trust should be imposed upon all unlawful or inequitable sums received by 21<sup>st</sup> Century Oncology traceable to Plaintiff and Class members.

**VIII. PRAYER FOR RELIEF**

Plaintiffs, on behalf of themselves and on behalf of the proposed Class and Subclass, request that the Court:

- a. Certify this case as a class action, appoint Plaintiffs as representatives of the Class and the Subclass, and appoint Plaintiffs' counsel to represent the Class and Subclass;
- b. Find that 21<sup>st</sup> Century Oncology breached its duty to safeguard and protect the PII of Plaintiff and the Class and Subclass members that was compromised in the Data Breach;
- c. Award Plaintiffs and Class and Subclass members appropriate relief, including actual and statutory damages, restitution and disgorgement;
- d. Award equitable, injunctive and declaratory relief as may be appropriate;
- e. Award all costs, including experts' fees and attorneys' fees, and the costs of prosecuting this action;
- f. Award pre-judgment and post-judgment interest as prescribed by law; and
- g. Grant additional legal or equitable relief as this Court may find just and proper.

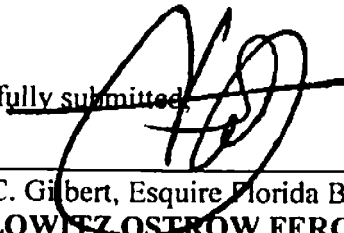
**IX. JURY TRIAL DEMAND**

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

Dated: September 9, 2016.

Respectfully submitted,

/s/

  
Robert C. Gilbert, Esquire Florida Bar No. 561861  
**KOPELOWITZ OSTRROW FERGUSON  
WEISELBERG GILBERT**  
2800 Ponce de Leon Blvd., Suite 1100  
Coral Gables, FL 33134  
Telephone: (305) 529-8858  
Facsimile: (954) 525-4300  
gilbert@kolawyers.com

***Counsel for Plaintiffs Veneta Delucchi and  
Bradley Bernius***

Gretchen Freeman Cappio, *pro hac vice forthcoming*  
Cari Campen Laufenberg, *pro hac vice forthcoming*  
Amy N. L. Hanson, *pro hac vice forthcoming*  
**KELLER ROHRBACK L.L.P.**  
1201 Third Avenue, Suite 3200  
Seattle, WA 98101  
Telephone: (206) 623-1900  
Facsimile: (206) 623-3384  
gcappio@kellerrohrback.com  
claufenberg@kellerrohrback.com  
ahanson@kellerrohrback.com

***Counsel for Plaintiff Veneta Delucchi***

Daniel C. Girard, *pro hac vice forthcoming*  
Jordan Elias, *pro hac vice forthcoming*  
Esfand Y. Nafisi, *pro hac vice forthcoming*  
Linh G. Vuong, *pro hac vice forthcoming*  
**GIRARD GIBBS LLP**  
601 California Street, 14th Floor  
San Francisco, CA 94108  
Telephone: (415) 981-4800  
Facsimile: (415) 981-4866  
dcg@girardgibbs.com  
je@girardgibbs.com  
eyn@girardgibbs.com  
lgy@girardgibbs.com

***Counsel for Plaintiff Bradley Bernius***

# EXHIBIT A



STATE OF NH  
DEPT OF JUSTICE

2016 MAR -7 AM 10: 13

**BakerHostetler**

**Baker & Hostetler LLP**

45 Rockefeller Plaza  
New York, NY 10111

T 212.589.4200  
F 212 589.4201  
www.bakerlaw.com

Theodore J. Kobus III  
direct dial: 212.271.1504  
tkobus@bakerlaw.com

March 4, 2016

**VIA OVERNIGHT MAIL**

Attorney General Joseph Foster  
Office of the Attorney General  
33 Capitol St  
Concord, NH 03301

*Re: Incident Notification*

Dear Attorney General Foster:

21<sup>st</sup> Century Oncology ("21<sup>st</sup> Century") is committed to maintaining the privacy and security of its patients' information. On November 13, 2015, the Federal Bureau of Investigation advised 21<sup>st</sup> Century that patient information was illegally obtained by an unauthorized third party who may have gained access to a 21<sup>st</sup> Century database. 21<sup>st</sup> Century immediately hired a leading forensics firm to support the investigation, assess 21<sup>st</sup> Century's systems and bolster security. The forensics firm determined that, on October 3, 2015, the intruder may have accessed the database, which contained information that included patients' names, Social Security numbers, physicians' names, diagnosis and treatment information, and insurance information.

The FBI asked 21<sup>st</sup> Century to delay notification or public announcement of the incident until now so as not to interfere with its investigation. 21<sup>st</sup> Century has no indication that patient information has been misused in any way. Out of an abundance of caution, however, today, 21<sup>st</sup> Century mailed letters to 1,202 New Hampshire residents pursuant to the requirements of the Health Insurance Portability and Accountability Act ("HIPAA"), in substantially the same form as the letter attached hereto.<sup>1</sup>

21<sup>st</sup> Century continues to work closely with the FBI on its investigation. In addition to security measures already in place, 21<sup>st</sup> Century has also taken steps to enhance internal security protocols to help prevent a similar incident in the future.

---

<sup>1</sup> As 21<sup>st</sup> Century does not conduct business in New Hampshire this letter is not, and does not constitute, a waiver of personal jurisdiction.

Atlanta Chicago Cincinnati Cleveland Columbus Costa Mesa Denver  
Houston Los Angeles New York Orlando Philadelphia Seattle Washington, DC

3

Joseph Foster  
March 4, 2016  
Page 2

Please do not hesitate to contact me if you have any questions regarding this matter.

Sincerely,

A handwritten signature in black ink, appearing to read "Theodore J. Kobus III". The signature is written in a cursive style with a large, stylized initial 'T'.

Theodore J. Kobus III

Enclosure



Return Mail Processing Center  
PO Box 6336  
Portland, OR 97228-6336

<<mail id>>  
<<First Name>><<Last Name>>  
<<Address1>>  
<<City>><<State>><<Zip>>

<<Date>>

Dear <<First Name>> <<Last Name>>:

21<sup>st</sup> Century Oncology is committed to maintaining the privacy and security of our patients' personal information. Regrettably, we are writing to inform you of an incident involving some of that information.

On November 13, 2015, the Federal Bureau of Investigation (FBI) advised us that patient information was illegally obtained by an unauthorized third party who may have gained access to a 21<sup>st</sup> Century database. We immediately hired a leading forensics firm to support our investigation, assess our systems and bolster security. The forensics firm determined that, on October 3, 2015, the intruder may have accessed the database, which contained information that may have included your name, Social Security number, physician's name, diagnosis and treatment information, and insurance information. We have no evidence that your medical record was accessed.

The FBI asked that we delay notification or public announcement of the incident until now so as not to interfere with its investigation. Now that law enforcement's request for delay has ended, we are notifying patients as quickly as possible. We continue to work closely with the FBI on its investigation of the intrusion into our system. In addition to security measures already in place, we have also taken steps to enhance internal security protocols to help prevent a similar incident in the future.

We have no indication that your information has been misused in any way; however, out of an abundance of caution, we are offering you a free one-year membership of Experian's<sup>®</sup> ProtectMyID<sup>®</sup> Alert. This product helps detect possible misuse of your personal information and provides you with identity protection services focused on immediate identification and resolution of identity theft. ProtectMyID Alert is completely free to you, and enrolling in this program will not hurt your credit score. For more information on identity theft prevention and ProtectMyID Alert, including instructions on how to activate your complimentary one-year membership, please see the additional information provided in this letter. We also recommend that you regularly review the explanation of benefits that you receive from your health insurer. If you see services that you did not receive, please contact your insurer immediately.

We deeply regret any concern this may cause you, and we want to emphasize that your care will not be affected by this incident. Should you have any questions, please call 1-866-446-1405, from 9 a.m. to 9 p.m. Eastern Time, Monday through Friday.

Sincerely,

A handwritten signature in black ink, appearing to read "Daniel Dosoretz".

Daniel Dosoretz, M.D.  
President and CEO

Attachment

**Activate ProtectMyID Now in Three Easy Steps**

1. ENSURE That You Enroll By: July 7, 2016 (Your code will not work after this date.)
2. VISIT the ProtectMyID Website to enroll: [www.protectmyid.com/redeem](http://www.protectmyid.com/redeem)
3. PROVIDE Your Activation Code: <<code>>

If you have questions or need an alternative to enrolling online, please call (866) 271-3084 and provide engagement #: PC98965

**ADDITIONAL DETAILS REGARDING YOUR 12-MONTH PROTECTMYID MEMBERSHIP:**

A credit card is not required for enrollment.

Once your ProtectMyID membership is activated, you will receive the following features:

- **Free copy of your Experian credit report**
- **Surveillance Alerts for:**
  - **Daily Bureau Credit Monitoring:** Alerts of key changes and suspicious activity found on your Experian, Equifax®, and TransUnion® credit reports.
- **Identity Theft Resolution and ProtectMyID ExtendCARE:** Toll-free access to U.S.-based customer care and a dedicated Identify Theft Resolution agent who will walk you through the process of fraud resolution from start to finish for seamless service. They will investigate each incident; help with contacting credit grantors to dispute charges and close accounts, including credit, debit, and medical insurance cards; assist with freezing credit files; and contact government agencies.
  - It is recognized that identity theft can happen months and even years after a data breach. To offer added protection, you will receive ExtendCARE™, which provides you with the same high level of Fraud Resolution support even after your ProtectMyID membership has expired.
- **\$1 Million Identity Theft Insurance\*:** Immediately covers certain costs, including lost wages, private investigator fees, and unauthorized electronic fund transfers.

**Activate your membership today at [www.protectmyid.com/redeem](http://www.protectmyid.com/redeem) or call (866) 271-3084 to register with the activation code above.**

Once your enrollment in ProtectMyID is complete, you should carefully review your credit report for inaccurate or suspicious items. If you have any questions about ProtectMyID, need help understanding something on your credit report, or suspect that an item on your credit report may be fraudulent, please contact Experian's customer care team at (866) 271-3084.

Even if you choose not to take advantage of this free credit monitoring service, we recommend that you remain vigilant to the possibility of fraud and identity theft by reviewing your credit card, bank, and other financial statements for any unauthorized activity. You may also obtain a copy of your credit report, free of charge, directly from each of the three nationwide credit reporting agencies. To order your credit report, free of charge, once every twelve months, please visit [www.annualcreditreport.com](http://www.annualcreditreport.com) or call toll-free at 1-877-322-8228. Contact information for the three nationwide credit reporting agencies is as follows:

Equifax  
PO Box 740241  
Atlanta, GA 30374  
[www.equifax.com](http://www.equifax.com)  
1-800-685-1111

Experian  
PO Box 2002  
Allen, TX 75013  
[www.experian.com](http://www.experian.com)  
1-888-397-3742

TransUnion  
PO Box 1000  
Chester, PA 19022  
[www.transunion.com](http://www.transunion.com)  
1-800-916-8800

If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Office of the Attorney General in your home state. Contact information for the Federal Trade Commission is as follows:

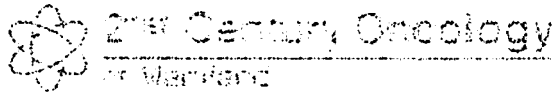
Federal Trade Commission  
600 Pennsylvania Avenue, NW  
Washington, D.C. 20580  
[www.ftc.gov/idtheft](http://www.ftc.gov/idtheft)  
1-877-438-4338

-

You can obtain information from these sources about steps an individual can take to avoid identity theft as well as information about fraud alerts and security freezes. You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records.

\* Identity theft insurance is underwritten by insurance company subsidiaries or affiliates of AIG. The description herein is a summary, intended for informational purposes only, and does not include all terms, conditions, and exclusions of the policies described. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

# EXHIBIT B



OFFICE OF THE ATTORNEY GENERAL

2013 JUL 10 AM 10:28

21st Century Oncology  
10000 Rockledge Drive

CERTIFIED MAIL – 7012 1010 0002 4846 2750  
RETURN RECEIPT REQUESTED

July 10, 2013

Office of the Attorney General  
Attn: Security Breach Notification  
200 St. Paul Place  
Baltimore, MD 21202

Dear Sir or Madam:

In accordance with MD Code, Com. Law § 14-3504(h), we are writing to inform you that on May 15, 2013 we learned from federal law enforcement officials that an employee of 21<sup>st</sup> Century Oncology Services, Inc., an affiliate of Peninsula Cancer Care Center and 21<sup>st</sup> Century Oncology of Maryland, has been criminally charged for having improperly accessed the personal health information of several of our patients, including two (2) patients from Maryland.

Based on the felony indictment against the former employee, we believe that the personal health information was improperly accessed between October 11, 2011 and August 8, 2012. Also based on the indictment, we have reason to believe that the individual obtained the name, social security number, and date of birth of these patients, and shared this information with a third party, who used it and/or intended to use it in order to file fraudulent tax returns with the Internal Revenue Service.

The employee in question is no longer employed by 21<sup>st</sup> Century Oncology Services, Inc. In addition, we are cooperating fully in the ongoing federal investigation of this matter, and we are also conducting our own internal investigation to determine how the employee was able to improperly access the patients' personal information.

We have established a toll-free number that patients can call if they believe their information has been misused. We are also offering individuals whose information was improperly accessed one year of credit monitoring service at no cost.


Please find enclosed a sample copy of the breach notice that we intend to send to these Maryland patients. In accordance with the Public Information Protection Act, the letter includes the following information:

- a description of the compromised information;
- contact information for our Privacy Officer via a toll-free number.
- toll-free numbers and addresses for Equifax, Experian and TransUnion;
- toll-free numbers, addresses and Websites for the Federal Trade Commission (FTC) and the Office of the Attorney General (OAG); and
- a statement that the individual can obtain information from these sources about steps to avoid identity theft.

While we believe this notice is compliant with the standards established by the Public Information Protection Act, regardless of this fact please note that it also meets the standards for breach notifications established under the Health Insurance Portability and Accountability Act of 1996 and the HITECH Act by the United States Department of Health and Human Services, Office for Civil Rights, which is our primary and functional federal regulator regarding privacy and security matters.

Please contact me if you have any questions in regard to this notice.

Sincerely,



Andrea L. Britt  
Privacy and Security Officer

Enclosures



July \_\_\_\_, 2013

«AddressBlock»

«GreetingLine»

Protecting our patients' personal information is a priority at 21<sup>st</sup> Century Oncology of Maryland d/b/a Peninsula Cancer Care Center, and we take any potential misuse of our patients' private health information very seriously. Unfortunately, we are writing to inform you that despite having a system in place to protect your personal information, we learned from federal law enforcement officials on May 15, 2013 that an employee of 21<sup>st</sup> Century Oncology Services, Inc., an affiliate of Peninsula Cancer Care Center, was being criminally charged for having improperly accessed your personal information.

Although it is not yet clear if or how this crime was perpetrated on both of us, we are doing everything possible to address this situation. The employee in question is no longer employed by 21<sup>st</sup> Century Oncology Services, Inc. We are cooperating fully in the government's ongoing investigation, and we are also conducting our own internal investigation to determine how the employee was able to access your personal information.

Based on the felony indictment against the former employee, we believe that your personal information was accessed between October 11, 2011 and August 8, 2012. Also based on the indictment, we have reason to believe that the individual obtained your name, social security number, and date of birth and shared this information with a third party, who used it and/or intended to use it in order to file fraudulent tax returns with the Internal Revenue Service.

If you think your personal information has been otherwise misused, please call 1-866-679-8944 so that we can investigate and provide that information to federal law enforcement officials investigating this matter.

In addition, in order to allow you to monitor your credit, we are also offering you one year of credit monitoring service at no cost.

Complimentary Three-Bureau Credit Monitoring Service

We have arranged for you to enroll in a three-bureau credit monitoring service called "My TransUnion Monitoring." The service is provided by TransUnion Interactive, one of the three nationwide credit reporting companies.

*To enroll in this free service online:*

1. Go to the TransUnion Monitoring website at [www.transunionmonitoring.com](http://www.transunionmonitoring.com);
2. In the space referenced as "Activation Code", enter the following unique 12-letter Activation Code: [ \_\_\_\_\_ ]
3. Then follow the simple steps to receive your credit monitoring service online.

*To enroll in this free service by mail:*

If you do not have access to the Internet or if you simply prefer paper-based services, you may enroll by completing the attached Credit Monitoring Authorization Form and mailing or faxing it back to TransUnion. Their address and fax number are provided on the form. After you have been enrolled in the paper-based service, TransUnion will send you credit updates by U.S. Priority Mail.

Due to privacy laws, we cannot register you directly. However, you can sign up for the online or offline credit monitoring service anytime between now and August 15, 2013. Please note that credit monitoring services might not be available for individuals that do not have a credit file with TransUnion, or an address in the United States (or its territories) or a valid Social Security number.

Other Resources

Please note that, as required by Maryland law, we also provided notice of this event to the Maryland Office of the Attorney General prior to sending you this notice. In addition, also in accordance with Maryland law, we are notifying you that the following available resources can provide additional information about preventing identity theft.

***Credit Reporting Agencies***

Experian  
955 American Lane  
Schaumburg, IL 60173  
<http://www.experian.com/>  
1-888-397-3742

Equifax  
Equifax Credit Information Services, Inc  
P.O. Box 740241  
Atlanta, GA 30374  
<http://www.equifax.com>  
1-888-766-0008

TransUnion  
TransUnion LLC  
P.O. Box 6790  
Fullerton, CA 92834  
<https://fraud.transunion.com>  
800-680-7289

***Government Resources***

Office of the Attorney General  
200 St. Paul Place  
Baltimore, MD 21202  
<http://www.oag.state.md.us/index.htm>  
1-888-743-0023

The Federal Trade Commission  
600 Pennsylvania Avenue, NW  
Washington, DC 20580  
<http://ftc.gov/>  
1-877-438-4338

We sincerely regret that this criminal action was allegedly taken by one of our employees. We are committed to insuring patient's information is protected and secure. Unfortunately, even the best systems cannot prevent all forms of criminal conduct. Nonetheless, we are reviewing our security procedures as result of this incident and will take any appropriate actions revealed by our investigation or the government's investigation of this matter.

In addition, as these investigations unfold, we will notify you if we learn any additional material information that affects you or your personal information. In the interim, if you have any questions, please feel free to contact me toll free at 1-866-679-8944.

Sincerely,

Andrea L. Britt  
Privacy and Security Officer



**TransUnion Authorization Form**

**Request for Offline, paper-based, TransUnion Three-Bureau Credit Monitoring Service**

**Directions:**

- ▶ Please print clearly and complete all fields
- ▶ Return signed and completed form to TransUnion by October 15, 2013

**Mail or Fax to:**

TransUnion  
1561 E. Orangethoke Ave., Suite 100  
Fullerton, CA 92831  
Fax: (714) 680-7201

Offer ID: B24638 [21st Century Oncology]

**Personal Information**

**First Name**

**Middle Name**

**Last Name**

**Suffix (JR, SR, II, III, IV, etc.)**

**Home Phone Number**

**Alternate Phone Number**

**Social Security Number**

**Activation Code "Required Field" Reference Notification Letter**

**Address Information**

**Street Address**

**Apt. or Unit Number**

**City**

**State**

**Zip Code**

I am submitting this authorization to TransUnion to start my enrollment, at no cost to me, in an offline paper-based TransUnion Three-Bureau Credit Monitoring Service, via U.S. Mail, which includes daily monitoring of my credit files at TransUnion, Experian and Equifax for a period of one year. I also certify that I am the person named above and that I am submitting this authorization to receive my TransUnion credit report and credit score for my personal review. I authorize TransUnion Interactive to access my credit data at TransUnion, Experian and Equifax.

Signature: \_\_\_\_\_

Date: \_\_\_\_\_

Check here if you would like TransUnion to add an initial 90-day "Fraud Alert" to your credit report which requests creditors to contact you before issuing credit.

Offer ID: B24638

JS 44 (Rev. 11/15)

### CIVIL COVER SHEET

The JS 44 civil cover sheet and the information contained herein neither replace nor supplement the filing and service of pleadings or other papers as required by law, except as provided by local rules of court. This form, approved by the Judicial Conference of the United States in September 1974, is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. (SEE INSTRUCTIONS ON NEXT PAGE OF THIS FORM.)

**I. (a) PLAINTIFFS**

Veneta Delucchi and Bradley Bernius, individually and on behalf of all others similarly situated

(b) County of Residence of First Listed Plaintiff **San Joaquin**  
(EXCEPT IN U.S. PLAINTIFF CASES)

(c) Attorneys (Firm Name, Address and Telephone Number)  
**Robert C. Gilbert, Kopelowitz Ostrow Ferguson Weisberg Gilbert**  
2800 Ponce de Leon Blvd., Suite 1100, Coral Gables, FL 33134  
Tel: (305) 529-8858 / Fax: (954) 525-4300

**DEFENDANTS**

21st Century Oncology Holdings, Inc.

**2016 SEP -9 PM 1:54**

County of Residence of First Listed Defendant **Lee**  
(IN U.S. PLAINTIFF CASES ONLY)

NOTE: IN LAND CONDEMNATION CASES, USE THE LOCATION OF THE TRACT OF LAND INVOLVED.

Attorneys (If Known)

**II. BASIS OF JURISDICTION** (Place an "X" in One Box Only)

- 1 U.S. Government Plaintiff
- 2 U.S. Government Defendant
- 3 Federal Question (U.S. Government Not a Party)
- 4 Diversity (Indicate Citizenship of Parties in Item III)

**III. CITIZENSHIP OF PRINCIPAL PARTIES** (Place an "X" in One Box for Plaintiff and One Box for Defendant)

- |   |                                       |                            |   |                            |                                       |
|---|---------------------------------------|----------------------------|---|----------------------------|---------------------------------------|
|   | PTF                                   | DEF                        |   | PTF                        | DEF                                   |
| Citizen of This State                   | <input type="checkbox"/> 1            | <input type="checkbox"/> 1 | Incorporated or Principal Place of Business in This State     | <input type="checkbox"/> 4 | <input checked="" type="checkbox"/> 4 |
| Citizen of Another State                | <input checked="" type="checkbox"/> 2 | <input type="checkbox"/> 2 | Incorporated and Principal Place of Business in Another State | <input type="checkbox"/> 5 | <input type="checkbox"/> 5            |
| Citizen or Subject of a Foreign Country | <input type="checkbox"/> 3            | <input type="checkbox"/> 3 | Foreign Nation  | <input type="checkbox"/> 6 | <input type="checkbox"/> 6            |

**IV. NATURE OF SUIT** (Place an "X" in One Box Only)

CONTRACT	TORTS	FORFEITURE/PENALTY	BANKRUPTCY	OTHER STATUTES
<input type="checkbox"/> 110 Insurance <input type="checkbox"/> 120 Marine <input type="checkbox"/> 130 Miller Act <input type="checkbox"/> 140 Negotiable Instrument <input type="checkbox"/> 150 Recovery of Overpayment & Enforcement of Judgment <input type="checkbox"/> 151 Medicare Act <input type="checkbox"/> 152 Recovery of Defaulted Student Loans (Excludes Veterans) <input type="checkbox"/> 153 Recovery of Overpayment of Veteran's Benefits <input type="checkbox"/> 160 Stockholders' Suits <input checked="" type="checkbox"/> 190 Other Contract <input type="checkbox"/> 195 Contract Product Liability <input type="checkbox"/> 196 Franchise	<b>PERSONAL INJURY</b> <input type="checkbox"/> 310 Airplane <input type="checkbox"/> 315 Airplane Product Liability <input type="checkbox"/> 320 Assault, Libel & Slander <input type="checkbox"/> 330 Federal Employers' Liability <input type="checkbox"/> 340 Marine <input type="checkbox"/> 345 Marine Product Liability <input type="checkbox"/> 350 Motor Vehicle <input type="checkbox"/> 355 Motor Vehicle Product Liability <input type="checkbox"/> 360 Other Personal Injury <input type="checkbox"/> 362 Personal Injury - Medical Malpractice	<input type="checkbox"/> 365 Personal Injury - Product Liability <input type="checkbox"/> 367 Health Care/Pharmaceutical Personal Injury Product Liability <input type="checkbox"/> 368 Asbestos Personal Injury Product Liability <b>PERSONAL PROPERTY</b> <input type="checkbox"/> 370 Other Fraud <input type="checkbox"/> 371 Truth in Lending <input type="checkbox"/> 380 Other Personal Property Damage <input type="checkbox"/> 385 Property Damage Product Liability	<input type="checkbox"/> 422 Appeal 28 USC 158 <input type="checkbox"/> 423 Withdrawal 28 USC 157 <b>PROPERTY RIGHTS</b> <input type="checkbox"/> 820 Copyrights <input type="checkbox"/> 830 Patent <input type="checkbox"/> 840 Trademark <b>LABOR</b> <input type="checkbox"/> 710 Fair Labor Standards Act <input type="checkbox"/> 720 Labor/Management Relations <input type="checkbox"/> 740 Railway Labor Act <input type="checkbox"/> 751 Family and Medical Leave Act <input type="checkbox"/> 790 Other Labor Litigation <input type="checkbox"/> 791 Employee Retirement Income Security Act <b>IMMIGRATION</b> <input type="checkbox"/> 462 Naturalization Application <input type="checkbox"/> 465 Other Immigration Actions	<input type="checkbox"/> 375 False Claims Act <input type="checkbox"/> 376 Qui Tam (31 USC 3729(a)) <input type="checkbox"/> 400 State Reapportionment <input type="checkbox"/> 410 Antitrust <input type="checkbox"/> 430 Banks and Banking <input type="checkbox"/> 450 Commerce <input type="checkbox"/> 460 Deportation <input type="checkbox"/> 470 Racketeer Influenced and Corrupt Organizations <input type="checkbox"/> 480 Consumer Credit <input type="checkbox"/> 490 Cable/Sat TV <input type="checkbox"/> 850 Securities Commodities/Exchange <input type="checkbox"/> 890 Other Statutory Actions <input type="checkbox"/> 891 Agricultural Acts <input type="checkbox"/> 893 Environmental Matters <input type="checkbox"/> 895 Freedom of Information Act <input type="checkbox"/> 896 Arbitration <input type="checkbox"/> 899 Administrative Procedure Act/Review or Appeal of Agency Decision <input type="checkbox"/> 950 Constitutionality of State Statutes
<b>REAL PROPERTY</b> <input type="checkbox"/> 210 Land Condemnation <input type="checkbox"/> 220 Foreclosure <input type="checkbox"/> 230 Rent Lease & Ejectment <input type="checkbox"/> 240 Torts to Land <input type="checkbox"/> 245 Tort Product Liability <input type="checkbox"/> 290 All Other Real Property	<b>CIVIL RIGHTS</b> <input type="checkbox"/> 440 Other Civil Rights <input type="checkbox"/> 441 Voting <input type="checkbox"/> 442 Employment <input type="checkbox"/> 443 Housing/Accommodations <input type="checkbox"/> 445 Amer. w/Disabilities - Employment <input type="checkbox"/> 446 Amer. w/Disabilities - Other <input type="checkbox"/> 448 Education	<b>PRISONER PETITIONS</b> <b>Habeas Corpus:</b> <input type="checkbox"/> 463 Alien Detainee <input type="checkbox"/> 510 Motions to Vacate Sentence <input type="checkbox"/> 530 General <input type="checkbox"/> 535 Death Penalty <b>Other:</b> <input type="checkbox"/> 540 Mandamus & Other <input type="checkbox"/> 550 Civil Rights <input type="checkbox"/> 555 Prison Condition <input type="checkbox"/> 560 Civil Detainee - Conditions of Confinement	<b>SOCIAL SECURITY</b> <input type="checkbox"/> 861 HIA (1395f) <input type="checkbox"/> 862 Black Lung (923) <input type="checkbox"/> 863 DIWC/DIWW (405(g)) <input type="checkbox"/> 864 SSID Title XVI <input type="checkbox"/> 865 RSI (405(g)) <b>FEDERAL TAX SUITS</b> <input type="checkbox"/> 870 Taxes (U.S. Plaintiff or Defendant) <input type="checkbox"/> 871 IRS—Third Party 26 USC 7609	

**V. ORIGIN** (Place an "X" in One Box Only)

- 1 Original Proceeding
- 2 Removed from State Court
- 3 Remanded from Appellate Court
- 4 Reinstated or Reopened
- 5 Transferred from Another District (specify)
- 6 Multidistrict Litigation

**VI. CAUSE OF ACTION**

Cite the U.S. Civil Statute under which you are filing (Do not cite jurisdictional statutes unless diversity):  
**28 U.S.C. § 1332(d)(2)**

Brief description of cause:  
**Failure to safeguard medical and other personal identifying information**

**VII. REQUESTED IN COMPLAINT:**

CHECK IF THIS IS A CLASS ACTION UNDER RULE 23, F.R.Cv.P.

DEMAND \$ **5,000,000.00**

CHECK YES only if demanded in complaint:  
JURY DEMAND:  Yes  No

**VIII. RELATED CASE(S) IF ANY**

(See instructions.)

JUDGE **Unassigned**

DOCKET NUMBER **2:16-cv-00210-UA-MRM**

DATE **09/09/2016**

SIGNATURE OF ATTORNEY OF RECORD

**FOR OFFICE USE ONLY**

RECEIPT #

AMOUNT **\$400**

APPLYING IFP

JUDGE

MAG. JUDGE

*(F-14409906)*

*2:16cv095f+m*

# ClassAction.org

This complaint is part of ClassAction.org's searchable class action lawsuit database and can be found in this post: [Lawuit Filed Against 21st Century Oncology Over 2015 Data Breach](#)

---