UNITED STATES DISTRICT COURT
MIDDLE DISTRICT OF FLORIDA
TAMPA DIVISION

IN RE: 21st CENTURY ONCOLOGY CUSTOMER DATA SECURITY BREACH LITIGATION	Case No. 8:16-md-2737-MSS-AEP MDL No. 2737
This Document Relates to All Cases	**AMENDED CONSOLIDATED CLASS ACTION COMPLAINT** **FILED UNDER SEAL**

TABLE OF CONTENTS

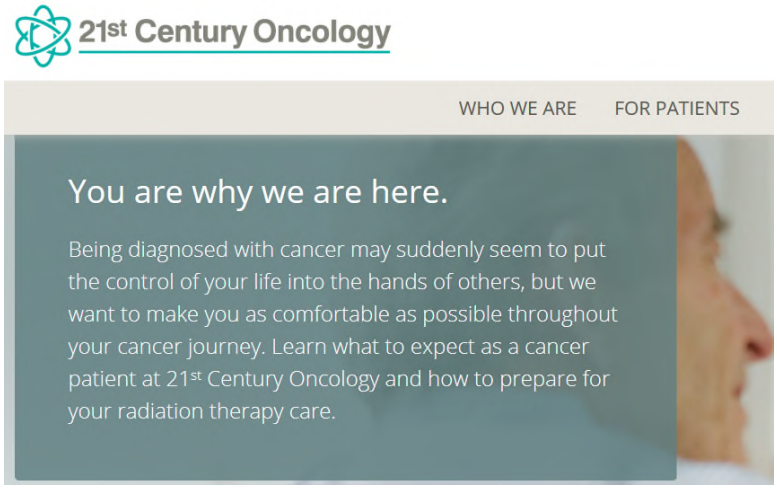
PAGE

I. INTRODUCTION

Plaintiffs,[1] individually and on behalf of all others similarly situated ("Class members"), file this Amended Consolidated Class Action Complaint against 21st Century Oncology Investments, LLC and 21st Century Oncology of California, a Medical Corporation (collectively "Defendants" or "21st Century"), 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 medical patient, survivor, or loved one can attest—and 21st Century recognizes on its website[2]—medical challenges are stressful and difficult, and a cancer diagnosis especially seems to place one's life out of control:



2. The last thing patients dealing with potentially deadly illnesses need is further

[1] "Plaintiffs" refers collectively to Plaintiffs Matthew Benzion, Steven Brehio, Judy Cabrera, Valerie Corbel, Veneta Delucchi, Jackie Griffith, Roxanne Haatvedt, Kathleen LaBarge, Sharon MacDermid, Timothy Meulenberg, Robert Russell, Carl Schmitt, Stacey Schwartz, and Stephen Wilbur.

[2] 21st Century, *What to Expect as a Cancer Patient*, https://www.21co.com/radiation-therapy/what-to-expect (last visited July 26, 2018).

harm and stress caused by the release, disclosure, and publication of their most private information, allowing it to be used by thieves.

3. But that is exactly what victims of a data breach that occurred at 21st Century on or around October 3, 2015 ("Data Breach") are enduring nationwide. Millions of 21st Century Data Breach victims have lost control of sensitive information that endangers their financial, medical, and emotional well-being for the rest of their lives. Plaintiffs are Data Breach victims and bring this proposed class action lawsuit on behalf of themselves and all other persons whose personally identifiable information ("PII") and protected health information ("PHI") have been compromised and made publicly accessible as a result of the 21st Century Data Breach (the "Class").

4. While more than 2.2 million 21st Century Data Breach victims sought out and/or paid for medical care from Defendants, thieves were hard at work, stealing and using their hard-to-change Social Security numbers and highly sensitive PII/PHI for over five months without the victims' knowledge. As a result of 21st Century's lax security practices, 21st Century impermissibly released, disclosed, and published Class members' PII/PHI by allowing this intrusion, which has worsened Plaintiffs' and other Class members' lives by, among other injuries: (a) adding to their already heightened financial obligations by placing them at increased risk of fraudulent charges; (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; and/or (c) increasing the risk of other personal, professional, or financial harms that could be caused as a result of having their PII/PHI made publicly accessible.

5. On or around October 3, 2015, for a period of several months or more, unauthorized parties illegally obtained patient information 21st Century made available on its provider database.[3] On account of 21st Century's failure to have implemented sufficient security protocols, 21st Century failed to detect the Data Breach until the Federal Bureau of Investigation ("FBI") notified it on or about November 13, 2015.[4]

6. The Data Breach resulted in the release, disclosure, and publication of private and highly sensitive PII/PHI including: names, Social Security numbers, physicians' names, medical diagnoses, treatment information, and insurance information.[5]

7. 21st Century is not a name known to all Class members, because 21st Century operates numerous facilities throughout the country under different trade names. In fact, some Class members were surprised and alarmed to learn that 21st Century—a company they were not familiar with—had access to their PII/PHI at all, much less had lost control of their PII/PHI and impermissibly released and disclosed it to unauthorized parties who could further publish and distribute their private and sensitive PII/PHI to anyone and everyone, including identity thieves.

8. Prior to the Data Breach, 21st Century acknowledged in the Notice of Privacy Practices 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

---

[3] 21st Century, *Notice to Patients Regarding Security Incident* (Mar. 4, 2016).
[4] *Id.*
[5] *Id.*

practices with respect to that protected health information, and to notify any affected individuals following a breach of any unsecured protected health information."[6] 21st Century also represented that it would abide by these obligations, but failed to live up to its own promises as well as its duties and obligations required by law and industry standards.

9. Contrary to its promises to help patients improve the quality of their lives, 21st Century's conduct has instead been a direct cause of the impermissible release, disclosure, and publication of Class members' PII/PHI, as well as the ongoing harm to Plaintiffs and other Class members whose suffering has been magnified by the Data Breach, and who will continue to experience harm and data insecurity for the indefinite future.

10. Specifically, 21st Century failed to maintain reasonable and/or adequate security measures to protect Plaintiffs' and other Class members' PII/PHI from being released, disclosed, and rendered publicly accessible to unauthorized parties, resulting in the publication of Plaintiffs' and other Class members' PII/PHI. In this regard, 21st Century's failures include, at a minimum: (1) the failure to maintain reasonable and adequate security measures designed to prevent the release, disclosure, and publication of Plaintiffs' PII/PHI, even though 21st Century had suffered from at least one previous data breach, and knew or should have known that it was a prized target for hackers; and (2) the failure to maintain reasonable and adequate security protocols to prevent and/or promptly detect the public accessibility of, unauthorized access of, and disclosure of PII/PHI from its provider database pertaining to 2.2 million 21st Century Data Breach victims.

---

[6] 21st Century, *Notice of Privacy Practices* (Mar. 26, 2013), https://www.21co.com/company/hipaa-notice-of-privacy-practices (last visited July 29, 2018).

11. While 21st Century had months to figure out how to protect and minimize harm to Plaintiffs and Class members from the Data Breach, its response was haphazard and ineffective. First, 21st Century caused additional harm to Plaintiffs and Class members through its delayed notification of the Data Breach. Adding insult to injury, it then offered only one year of credit monitoring and identity theft insurance, and provided only four months from notification of the Data Breach in which to sign up.

12. Moreover, credit monitoring and identity theft insurance alone do not eliminate the risk of identity theft and fraud. Even with such protections, Plaintiffs and Class members may still experience identity theft and then be required to spend significant time undoing the financial injury inflicted by identity thieves who seek to use compromised PII/PHI for financial gain.

13. In addition, credit monitoring fails to remedy the potentially life-threatening injury to Plaintiffs and other Class members inflicted by identity thieves who seek to use victims' compromised PII/PHI 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.

14. Having released, disclosed, and published Plaintiffs' and Class members' PII/PHI, 21st Century has rendered Plaintiffs' and Class members' PII/PHI publicly accessible and assured that identity thieves have access to Plaintiffs' and other Class members' compromised PII/PHI on an ongoing basis. PII/PHI such as Social Security numbers can be used indefinitely, because, unlike credit and financial accounts, these numbers are extremely difficult to change. In addition, medical identity theft can continue to

harm Plaintiffs and other Class members indefinitely, because this information is often shared amongst numerous providers. Further, as a consequence of the Data Breach, Plaintiffs and Class members are at increased risk of personal, professional, or financial harms that could be caused as a result of having their PII/PHI exposed, released, disclosed, and published.

15. Plaintiffs bring this proposed class action lawsuit on behalf of themselves and the Class. They seek damages, restitution, and injunctive relief requiring 21st Century to implement and maintain security practices to comply with regulations designed to prevent and remedy this and other potential data breaches, as well as other relief as the Court may order. Plaintiffs and Class members will have to remain vigilant for the rest of their lives to combat potential identity theft. Despite all best efforts of Plaintiffs, Class members, or anyone else, this most sensitive personal information can never be made private again.

III. JURISDICTION

16. 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, Defendants do business nationwide in 17 states, and members of the proposed Class are citizens of different states than Defendants.

17. This Court has personal jurisdiction over 21st Century, because 21st Century maintains its headquarters and principal executive and administrative offices in Florida and has sufficient minimum contacts with Florida.

18. Venue is proper in this district under 28 U.S.C. § 1391(b), because 21st Century resides in this district and a substantial part of the events or omissions giving rise to

Plaintiffs' claims occurred in this district. Venue is also appropriate in this district pursuant to United States Judicial Panel on Multidistrict Litigation's October 6, 2016 Transfer Order transferring and centralizing this case in the Middle District of Florida.

IV. PARTIES

A. Plaintiffs

Arizona

Plaintiff Robert Russell

19. Plaintiff Robert Russell is a citizen of and is domiciled in the state of Arizona. Plaintiff Russell is unable to determine how 21st Century obtained his confidential and sensitive PII/PHI.

20. In March 2016, Plaintiff Russell received notice from 21st Century that his PII/PHI had been compromised in the Data Breach.

21. Plaintiff Russell subsequently spent approximately 15 to 20 hours taking action to mitigate the impact of the Data Breach, including researching the Data Breach and 21st Century, reviewing credit reports and financial accounts for fraud or suspicious activity, reviewing medical statements for fraud or suspicious activity, researching and enrolling in the credit monitoring service offered by 21st Century, and contacting 21st Century, a government agency, and a medical insurer regarding the Data Breach. He now spends on average one hour a week reviewing credit monitoring reports and checking account statements for irregularities.

22. Since the one year of identity theft protection offered by 21st Century expired in approximately March 2017, Plaintiff Russell has purchased credit monitoring and identity

theft protection services through [redacted], for which he pays approximately $8 per month. He plans to purchase such services on an ongoing basis to protect himself from identity theft and fraud.

23. As a result of the Data Breach, Plaintiff Russell has suffered emotional distress as a result of the release of his PII/PHI, which he expected 21st Century to protect from disclosure, including anxiety, concern, and unease about unauthorized parties viewing and potentially using his personal and medical information. As a result of the Data Breach, Plaintiff Russell anticipates spending considerable time and money to contain the impact of the Data Breach.

California

Plaintiff Valerie Corbel

24. Plaintiff Valerie Corbel is a citizen of and is domiciled in the state of California. Plaintiff Corbel is the widow of James Corbel, who was a Plaintiff and proposed Class representative named in the Consolidated Complaint, filed in this action on January 17, 2017 (ECF No. 100).

25. James Corbel was a citizen of and was domiciled in the state of California. Plaintiff Corbel received medical services from 21st Century affiliates located in California and provided confidential and sensitive PII/PHI to 21st Century.

26. In March 2016, James Corbel received notice from 21st Century that his PII/PHI had been compromised in the Data Breach.

27. James Corbel subsequently spent approximately 10 hours taking action to mitigate the impact of the Data Breach, including requesting and reviewing a credit report,

and reviewing financial accounts for fraud or suspicious activity.

28. Despite James Corbel's efforts to protect himself, he began receiving suspicious telephone calls asking for money and/or James Corbel's personal information.

29. As a result of the Data Breach, James Corbel suffered emotional distress as a result of the release of his protected health information, which he expected 21st Century to protect from disclosure, including anxiety, concern, and unease about unauthorized parties viewing and potentially using his personal and medical information.

30. James Corbel died on May 3, 2017, during the pendency of this action.

31. Plaintiff Corbel filed a Statement of Fact of Death on May 8, 2017 (ECF No. 148).

32. James Corbel's death did not extinguish his claims in this action.

33. Plaintiff Corbel is James Corbel's successor, sole beneficiary, and representative of his estate.

Plaintiff Roxanne Haatvedt

34. Plaintiff Roxanne Haatvedt is a citizen of and is domiciled in the state of California. Plaintiff Haatvedt received medical services from an affiliate of 21st Century located in California and provided confidential and sensitive PII/PHI to Defendants.

35. In March 2016, Plaintiff Haatvedt received notice from 21st Century that her PII/PHI had been compromised in the Data Breach.

36. Plaintiff Haatvedt subsequently spent approximately 20 hours taking action to mitigate the impact of the Data Breach, including researching the Data Breach and 21st Century, reviewing credit reports and financial accounts for fraud or suspicious activity, and

researching and enrolling in the credit monitoring service offered by Defendants. She now spends on average four hours a month reviewing credit monitoring reports and checking account statements for irregularities.

37. Since the one year of identity theft protection offered by 21st Century expired in approximately March 2017, Plaintiff Haatvedt has purchased credit monitoring and identity theft protection services on an annual basis for approximately $90 a year. She recently renewed these services for a second year that expires on March 29, 2019. She plans to purchase such services on an ongoing basis to protect herself from identity theft and fraud.

38. As a result of the Data Breach, Plaintiff Haatvedt has suffered emotional distress as a result of the release of her PII/PHI, which she expected 21st Century to protect from disclosure, including anxiety, concern, and unease about unauthorized parties viewing and potentially using her personal and medical information. As a result of the Data Breach, Plaintiff Haatvedt anticipates spending considerable time and money to contain the impact of the Data Breach.

Plaintiff Veneta Delucchi

39. Plaintiff Veneta Delucchi is a citizen of and is domiciled in the state of California. Plaintiff Delucchi received medical services from an affiliate of 21st Century located in California and provided confidential and sensitive PII/PHI to Defendants.

40. In March 2016, Plaintiff Delucchi received notice from 21st Century that her PII/PHI had been compromised in the Data Breach.

41. Plaintiff Delucchi subsequently spent approximately 10 to 15 hours taking action to mitigate the impact of the Data Breach, including researching the Data Breach and

21st Century, reviewing financial accounts for fraud or suspicious activity, and researching and enrolling in the credit monitoring service offered by 21st Century. She now spends on average three hours a week reviewing credit monitoring reports and checking account statements for irregularities.

42. In approximately May 2017, Plaintiff Delucchi was the victim of identity theft, in which an unauthorized individual withdrew $300 cash from her checking account.

43. Since the one year of identity theft protection offered by 21st Century expired in approximately March 2017, Plaintiff Delucchi has purchased credit monitoring and identity theft protection services through [redacted], for which she pays approximately $17 per month. She plans to purchase such services on an ongoing basis to protect herself from identity theft and fraud.

44. As a result of the Data Breach, Plaintiff Delucchi has suffered emotional distress as a result of the release of her PII/PHI, which she expected 21st Century to protect from disclosure, including anxiety, concern, and unease about unauthorized parties viewing and potentially using her personal and medical information. As a result of the Data Breach, Plaintiff Delucchi anticipates spending considerable time and money to contain the impact of the Data Breach.

Florida

Plaintiff Carl Schmitt

45. Plaintiff Carl Schmitt is a citizen of and is domiciled in the state of Florida. Plaintiff Schmitt received medical services from a 21st Century affiliate located in Florida, and provided confidential and sensitive PII/PHI to 21st Century.

46. In January 2016, Plaintiff Schmitt discovered that his PII/PHI had been used by unauthorized parties to commit fraud. Plaintiff Schmitt received notifications from [redacted] and [redacted] that fraud was committed using his PII/PHI. For instance, Plaintiff Schmitt received notification from [redacted] that the address on his account was changed and that a request was made to send replacement credit cards to the new address. Plaintiff Schmitt also received notification from [redacted] that someone attempted to open an [redacted] credit card in his name and to order items using his account. Plaintiff Schmitt also received notification from [redacted] that an unauthorized party attempted to change his contact information. As a result, Plaintiff Schmitt's [redacted] credit card was cancelled, and a new credit card had to be issued to prevent unauthorized transactions.

47. Plaintiff Schmitt has also received numerous phishing emails. For example, he received a phishing email purporting to be from [redacted] asking that he provide certain information. Plaintiff Schmitt went to [redacted] which verified it was not an email sent by [redacted]. As a result, [redacted] cancelled Plaintiff Schmitt's credit card and issued him a new one. Plaintiff Schmitt also received notification from [redacted] that an unauthorized party attempted to change his contact information. Plaintiff Schmitt's credit card had to be cancelled, and a new credit card was issued to prevent unauthorized transactions. Between January 2016 to the present, Plaintiff Schmitt has received numerous other phishing emails from financial institutions, retailers, and utilities, including where he has existing accounts, at a rate much higher than he received prior to the Data Breach.

48. Plaintiff Schmitt subsequently spent over approximately 60 hours taking action to mitigate the impact of the Data Breach, corresponding and communicating with

[redacted], and other financial institutions, utilities, and retailers, as well as reviewing financial accounts for fraud or suspicious activities, contacting the FTC and the local police departments to report fraudulent activity, and placing credit freezes with Experian, Equifax and TransUnion.

49. In April 2016, Plaintiff Schmitt received notice from 21st Century that his PII/PHI had been compromised in the Data Breach.

50. Plaintiff Schmitt subsequently spent approximately 25 hours taking action to mitigate the impact of the Data Breach, including researching the Data Breach and 21st Century, and researching ways to protect himself from data breaches. He now spends on average one hour a month reviewing credit monitoring reports and checking account statements for irregularities.

51. As a result of the Data Breach, Plaintiff Schmitt has suffered emotional distress as a result of the release of his PII/PHI, which he expected 21st Century to protect from disclosure, including anxiety, concern, and unease about unauthorized parties viewing and potentially using his personal and medical information. As a result of the Data Breach, Plaintiff Schmitt anticipates spending considerable time and money to contain the impact of the Data Breach.

Plaintiff Matthew Benzion

52. Plaintiff Matthew Benzion is a citizen of and is domiciled in the state of Florida. Plaintiff Benzion received medical services from a 21st Century affiliate located in Florida and provided confidential and sensitive PII/PHI to 21st Century.

53. In March 2016, Plaintiff Benzion received notice from 21st Century that his

PII/PHI had been compromised in the Data Breach.

54. Plaintiff Benzion subsequently spent approximately 15 hours taking action to mitigate the impact of the Data Breach, including researching the Data Breach and 21st Century, researching ways to protect himself from data breaches, reviewing his financial accounts for fraud or suspicious activity, and enrolling in a credit monitoring service. He now spends on average one hour a month reviewing credit monitoring reports and checking account statements for irregularities.

55. As a result of the Data Breach, Plaintiff Benzion purchased [redacted], a credit monitoring service, for which he pays approximately $30 per month. He plans to purchase such services on an ongoing basis to protect himself from identity theft and fraud.

56. As a result of the Data Breach, Plaintiff Benzion has suffered emotional distress as a result of the release of his PII/PHI, which he expected 21st Century to protect from disclosure, including anxiety, concern, and unease about unauthorized parties viewing and potentially using his personal and medical information. As a result of the Data Breach, Plaintiff Benzion anticipates spending considerable time and money to contain the impact of the Data Breach.

Plaintiff Kathleen LaBarge

57. Plaintiff Kathleen LaBarge is a citizen of and is domiciled in the state of Florida. Plaintiff LaBarge received medical services from a 21st Century affiliate located in Florida and provided confidential and sensitive PII/PHI to Defendants.

58. In March 2016, Plaintiff LaBarge received notice from 21st Century that her

PII/PHI had been compromised in the Data Breach. She spends approximately one hour a month reviewing credit monitoring reports and checking account statements for irregularities.

59. Plaintiff LaBarge spends approximately $99 per year to obtain identity theft protection with [redacted]. She also spends approximately $80 per year to obtain identity theft protection through [redacted]. She plans to purchase such services on an ongoing basis to protect herself from identity theft and fraud.

60. As a result of the Data Breach, Plaintiff LaBarge has suffered emotional distress as a result of the release of her PII/PHI, which she expected 21st Century to protect from disclosure, including anxiety, concern, and unease about unauthorized parties viewing and potentially using her personal and medical information. As a result of the Data Breach, Plaintiff LaBarge anticipates spending considerable time and money to contain the impact of the Data Breach.

Plaintiff Stacey Schwartz

61. Plaintiff Stacey Schwartz is a citizen of and is domiciled in the state of Florida. He received medical services from an affiliate of Defendants located in Florida and provided confidential and sensitive PII/PHI to Defendants.

62. In March 2016, Plaintiff Schwartz received notice from 21st Century that his PII/PHI had been compromised in the Data Breach.

63. After receiving notice about the Data Breach, Plaintiff Schwartz spent approximately 13 hours taking action to mitigate the impact of the Data Breach, including (a) researching the Data Breach and Defendants; (b) contacting Defendants to inquire about the Data Breach and to confirm that the notice he received was not a scam; (c) reviewing his

financial accounts for fraud or suspicious activity; and (d) researching and ultimately enrolling in credit monitoring services with [redacted], for which he pays approximately $198 per year. He plans to purchase such services on an ongoing basis to protect himself from identity theft and fraud.

64. Despite Plaintiff Schwartz's efforts to protect himself, he discovered that his PII/PHI has been used by unauthorized parties to commit fraud. On April 25, 2016, Plaintiff Schwartz received an alert from [redacted] notifying him that an unknown third party had used his name, date of birth, and Social Security number to apply for a [redacted] credit card. He informed [redacted] and [redacted] that he did not submit this application. On September 30, 2016, October 1, 2016, and October 2, 2016, Plaintiff Schwartz received three separate notifications from [redacted] that, on August 1, 2016, an unknown third party had attempted to apply for a [redacted] credit card using his PII/PHI. Also, on or about December 27, 2017, Plaintiff Schwartz was notified that an unauthorized individual attempted to make a purchase totaling $3,490 using his [redacted] credit card, as a result of which Plaintiff Schwartz's credit card was cancelled, and he was issued a replacement credit card with a new account number.

65. Plaintiff Schwartz has spent approximately an additional 16 hours addressing the fraudulent activity, including (a) contacting [redacted] to inform them that he did not submit credit card applications; (b) filing a police report with the Miami police; (c) filing an online complaint with the Federal Bureau of Investigation; (d) contacting financial institutions with which he does business to add protection to his accounts and to discuss other options to protect himself and his accounts; (e) placing security freezes on his

credit with Experian, Equifax, and TransUnion, for which he paid $30; and (f) filing a complaint with the FTC. He now spends on average one hour a week reviewing credit monitoring reports and checking account statements for irregularities.

66. As a result of the Data Breach, Plaintiff Schwartz has suffered emotional distress as a result of the release of his PII/PHI, which he expected 21st Century to protect from disclosure, including anxiety, concern, and unease about unauthorized parties viewing and potentially using his personal and medical information. As a result of the Data Breach, Plaintiff Schwartz anticipates spending considerable time and money to contain the impact of the Data Breach.

Plaintiff Timothy Meulenberg

67. Plaintiff Timothy Meulenberg is a citizen of and is domiciled in the state of Florida. Plaintiff Meulenberg received medical services from Defendants located in Florida and provided confidential and sensitive PII/PHI to Defendants.

68. In March 2016, Plaintiff Meulenberg received notice from 21st Century that his PII/PHI had been compromised in the Data Breach.

69. Plaintiff Meulenberg subsequently spent approximately 30 hours taking action to mitigate the impact of the Data Breach, including contacting banks, credit card companies, the three major credit reporting agencies, the Social Security Administration, and the Internal Revenue Service. He now spends on average one hour a week reviewing credit monitoring reports and checking account statements for irregularities.

70. Plaintiff Meulenberg has also spent $30 to place credit freezes on his accounts with each of the three major credit-reporting agencies.

71. Despite Plaintiff Meulenberg's efforts to protect himself, he discovered that his PII/PHI had been used by unauthorized parties to commit fraud. On February 24, 2016, an attempt was made by unauthorized parties to open a [redacted] credit card account. Furthermore, on March 10, 2016, an attempt was made by unauthorized parties to open a [redacted] credit card account. Also, on or about November 2016, Plaintiff Meulenberg discovered unauthorized charges totaling $170 on his [redacted] credit card account. This card was cancelled and reissued. To combat further incidences of identity theft on open credit cards, Plaintiff Meulenberg now receives a text message whenever any money is charged to any of his credit card accounts. If and when a fraudulent charge is identified, Plaintiff Meulenberg is able to have the charge denied, freeze further use of the card in question, and obtain a new card from the issuer of the card.

72. Since the one year of identity theft protection offered by 21st Century expired in approximately March 2017, Plaintiff Meulenberg has acquired credit monitoring and identity theft protection services through [redacted] As a preferred customer of [redacted] credit monitoring and identity theft protection services are included as a provided service and as part of the service fees he pays. Notwithstanding his status as a preferred customer, on April 26, 2018, Plaintiff Meulenberg's [redacted] checking account was hacked, and funds were wired out of the account to an account overseas. Plaintiff Meulenberg intends to close this account.

73. Plaintiff Meulenberg has also received numerous phishing emails from approximately February 2016 to the present, at a rate much higher than the occasional phishing emails he received prior to the Data Breach.

74. As a result of the Data Breach, Plaintiff Meulenberg has suffered emotional distress as a result of the release of his PII/PHI, which he expected 21st Century to protect from disclosure, including anxiety, concern, and unease about unauthorized parties viewing and potentially using his personal and medical information. As a result of the Data Breach, Plaintiff Meulenberg anticipates spending considerable time and money to contain the impact of the Data Breach.

Plaintiff Stephen Wilbur

75. Plaintiff Stephen Wilbur is a citizen of and is domiciled in the state of Florida. Plaintiff Wilbur received medical services from a 21st Century affiliate located in Florida and provided confidential and sensitive PII/PHI to Defendants.

76. In January 2016, when Plaintiff Wilbur's wife attempted to pick up Plaintiff Wilbur's prescription, a [redacted] pharmacist informed her that Plaintiff Wilbur's health insurance coverage was not valid. Plaintiff Wilbur contacted his health insurance company to determine why his health insurance was invalid, and a representative informed him that it had been cancelled and that the company would commence an investigation. Plaintiff Wilbur learned through his health insurance agent that his Social Security number had been compromised. Because his Social Security number had been stolen, Plaintiff Wilbur's health insurance company was unable to reinstate his coverage under his Social Security number and had to create a fictitious Social Security number to create a new health insurance account under his name.

77. During the time he was without coverage, Plaintiff Wilbur's health insurance company denied his claims for medical services. As a result, he incurred out-of-pocket costs

of over $575. Additional out-of-pocket costs were only recouped after extensive delay and effort by Plaintiff Wilbur and his wife.

78. In March 2016, Plaintiff Wilbur received notice from 21st Century that his PII/PHI had been compromised in the Data Breach.

79. In November or December 2016, Plaintiff Wilbur received notice from the health insurance company that the Internal Revenue Service had rejected his fictitious number. Plaintiff Wilbur may be liable for tax penalties for "failure" to have health insurance coverage, for which Plaintiff Wilbur has had to provide proof. The Internal Revenue Service investigation is pending. On January 11, 2017, Plaintiff Wilbur's health insurance company informed him that it would notify the Social Security Administration that his Social Security number has been stolen.

80. Plaintiff Wilbur has spent approximately 75 to 80 hours addressing the fraudulent activity, including (a) contacting his health insurance company regarding the fraud; (b) communicating with his health insurance agent and attempting to reinstate his health insurance coverage; (c) searching for and obtaining alternative health insurance coverage that provides him less favorable and more expensive coverage; and (d) corresponding with the Internal Revenue Service regarding his health insurance coverage.

81. After receiving notice about the Data Breach, Plaintiff Wilbur spent an additional 75 to 80 hours taking action to mitigate further impact of the Data Breach, including (a) researching the Data Breach and Defendants; (b) attempting to contact Defendants to inquire about the Data Breach, to which Defendants have been unresponsive; (c) enrolling in credit monitoring services; (d) reviewing his credit report and financial

accounts for fraud or suspicious activity; (e) filing a complaint online with the FTC; and (f) notifying his Certified Public Accountant of the Data Breach.

82. As a result of the Data Breach, Plaintiff Wilbur has suffered emotional distress as a result of the release of his PII/PHI, which he expected 21st Century to protect from disclosure, including anxiety, concern, and unease about unauthorized parties viewing and potentially using his personal and medical information. As a result of the Data Breach, Plaintiff Wilbur anticipates spending considerable additional time and money to contain and try to mitigate further impact of the Data Breach.

Plaintiff Judy Cabrera

83. Plaintiff Judy Cabrera is a citizen of and is domiciled in the state of Florida. She received medical services from a 21st Century affiliate located in Florida and provided confidential and sensitive PII/PHI to Defendants.

84. In March 2016, Plaintiff Cabrera received notice from 21st Century that her PII/PHI had been compromised in the Data Breach.

85. After receiving notice about the Data Breach, Plaintiff Cabrera spent approximately 50 hours taking action to mitigate the impact of the Data Breach, including (a) researching the Data Breach; (b) reviewing her financial account and credit score daily for fraud or suspicious activity; (c) attempting to enroll in the free credit monitoring services offered in the Data Breach notice and finding that the services were no longer available; and (d) researching and ultimately enrolling in credit monitoring services with [redacted], for which she pays approximately $187 per year. She plans to purchase such services on an ongoing basis to protect herself from identity theft and fraud. She now spends on average

three hours a week reviewing credit monitoring reports and checking account statements for irregularities.

86. Despite Plaintiff Cabrera's efforts to protect herself, she discovered that her PII/PHI has been sold or traded by unauthorized parties. On January 15, 2017, Plaintiff Cabrera received an alert from [redacted] notifying her that her PII/PHI has been "given away, traded or sold" on the "Dark Web, Deep Web, or Peer-to-Peer File Sharing Networks."

87. As a result of the Data Breach, Plaintiff Cabrera has suffered emotional distress as a result of the release of her PII/PHI, which she expected 21st Century to protect from disclosure, including anxiety, concern, and unease about unauthorized parties viewing and potentially using her personal and medical information. As a result of the Data Breach, Plaintiff Cabrera anticipates spending considerable time and money to contain the impact of the Data Breach.

Kentucky

Plaintiff Jackie Griffith

88. Plaintiff Jackie Griffith is a citizen of and is domiciled in the state of Kentucky. Plaintiff Griffith received medical services from a 21st Century affiliate located in Kentucky and provided confidential and sensitive PII/PHI to Defendants.

89. In March 2016, Plaintiff Griffith received notice from 21st Century that her PII/PHI had been compromised in the Data Breach. After learning of the Data Breach, Plaintiff Griffith enrolled in the one-year membership with Experian's ProtectMyID Alert offered by 21st Century.

90. Plaintiff Griffith spent and continues to spend approximately two hours every

month taking action to mitigate the impact of the Data Breach and addressing the threat of fraudulent activity, including reviewing credit reports and financial accounts for fraud or suspicious activity.

91. Despite Plaintiff Griffith's efforts to protect herself, she discovered that her PII/PHI had been used by unauthorized parties to commit or attempt to commit fraud in 2016, when she received email notifications of fraudulent purchases made in her name on [redacted] Plaintiff Griffith knew this was suspicious because she had never shopped at [redacted] As a result, she spent time on the phone with [redacted] attempting to remedy the situation and prevent fraudulent purchases.

92. Also, in late March of 2016, [redacted] notified Plaintiff Griffith that an unauthorized party attempted to access her credit card. As a result, she spent time on the phone with the bank and changed her password.

93. Further, upon enrolling in [redacted], Plaintiff Griffith discovered that a collection agency had placed a false Tennessee address on her credit report, resulting in a "hold" on her credit. Plaintiff Griffith spent approximately 10 hours attempting to have this address removed from her credit report, incurred out-of-pocket costs of approximately $15 for copies and fax expenses, and made approximately eight round trips of approximately 13 miles to the local library, incurring mileage of approximately $7 for each trip.

94. Moreover, in July 2018, Plaintiff Griffith discovered that a hard inquiry was made on her credit for the purpose of signing up for [redacted], which she did not authorize. Plaintiff Griffith currently spends approximately 15 to 20 hours each month attempting to

remove this and other false information from her credit report.

95. As a result of the Data Breach, Plaintiff Griffith has suffered emotional distress as a result of the release of her PII/PHI, which she expected 21st Century to protect from disclosure, including anxiety, concern, and unease about unauthorized parties viewing and potentially using her personal and medical information. As a result of the Data Breach, Plaintiff Griffith anticipates spending considerable time and money to contain the further impact of the Data Breach.

New Jersey

Plaintiff Sharon MacDermid

96. Plaintiff Sharon MacDermid is a citizen of and is domiciled in the state of New Jersey. Plaintiff MacDermid received medical services from a division of 21st Century located in Florida and provided confidential and sensitive PII/PHI to Defendants.

97. In March 2016, Plaintiff MacDermid received notice from 21st Century that her PII/PHI had been compromised in the Data Breach.

98. Plaintiff MacDermid subsequently spent approximately 10 to 15 hours taking action to mitigate the impact of the Data Breach, including researching the Data Breach and 21st Century, reviewing financial accounts for fraud or suspicious activity, and researching how to protect herself from the consequences of the Data Breach. She now spends on average one hour a month reviewing credit monitoring reports and checking account statements for irregularities.

99. Plaintiff MacDermid pays approximately $30 per month for credit monitoring and identity theft protection services by [redacted]. She plans to purchase such services on an

ongoing basis to protect herself from identity theft and fraud.

100. As a result of the Data Breach, Plaintiff MacDermid has suffered emotional distress as a result of the release of her PII/PHI, which she expected 21st Century to protect from disclosure, including anxiety, concern, and unease about unauthorized parties viewing and potentially using her personal and medical information. As a result of the Data Breach, Plaintiff MacDermid anticipates spending considerable time and money to contain the impact of the Data Breach.

Rhode Island

Plaintiff Steven Brehio

101. Plaintiff Steven Brehio is a citizen of and is domiciled in the state of Rhode Island. Plaintiff Brehio received medical services from an affiliate of 21st Century Oncology located in Rhode Island and provided confidential and sensitive PII/PHI to 21st Century.

102. In March 2016, Plaintiff Brehio received notice from 21st Century that his PII/PHI had been compromised in the Data Breach. After learning of the Data Breach, Plaintiff Brehio enrolled in the one-year membership with [redacted] offered by 21st Century.

103. Since the one year of identity theft protection offered by 21st Century expired in approximately March 2017, Plaintiff Brehio has purchased credit monitoring and identity theft protection services through [redacted], for which he pays approximately $18 per month. He plans to purchase such services on an ongoing basis to protect himself from identity theft and fraud.

104. Despite Plaintiff Brehio's efforts to protect himself from fraud following the

Data Breach, he discovered that his PII/PHI had been used by unauthorized parties to commit fraud. Plaintiff Brehio was notified in approximately July 2016 by [redacted] that an account for two cell phones was opened in his name. Plaintiff Brehio received a bill from [redacted] for $282.83. Plaintiff Brehio was also notified in approximately July 2016 by [redacted] that his account was used fraudulently without his permission. Plaintiff Brehio was notified in approximately August 2016 that someone was using his name, Social Security number and date of birth to try to open a [redacted] credit card account in his name. Plaintiff Brehio has spent approximately 10 hours addressing the fraudulent activity, including contacting [redacted] and [redacted], filing reports with local police agencies and the Federal Trade Commission, reviewing his accounts, and placing credit freezes with Experian, Equifax and TransUnion.

105. Plaintiff Brehio also spent approximately 20 hours taking action to mitigate the impact of the Data Breach, including researching 21st Century and the Data Breach, reviewing financial accounts for fraudulent or suspicious activity, researching and enrolling in the credit monitoring service offered by 21st Century, contacting local police agencies and the FTC regarding fraudulent activities, and placing credit freezes with Experian, Equifax and TransUnion. He now spends on average one hour a month reviewing credit monitoring reports and checking account statements for irregularities.

106. Plaintiff Brehio has also made multiple trips totaling approximately 40 miles to provide information to local police agencies about the fraudulent activities on his accounts, incurring mileage of approximately $20.

107. As a result of the Data Breach, Plaintiff Brehio has suffered emotional distress as a result of the release of his PII/PHI, which he expected 21st Century to protect from

disclosure, including anxiety, concern, and unease about unauthorized parties viewing and potentially using his personal and medical information. As a result of the Data Breach, Plaintiff Brehio anticipates spending considerable time and money to contain the impact of the Data Breach. This includes weekly checks of personal and financial accounts and the extension of his credit freeze for at least seven years.

B. Defendants

108. Defendant 21st Century Oncology Investments, LLC is a Delaware limited liability company with its principal place of business in Ft. Myers, Florida. Defendant 21st Century Oncology Investments, LLC is the 100% owner of its subsidiary 21st Century Oncology Holdings, Inc., which in turn is the 100% owner of its subsidiary 21st Century Oncology, Inc., which in turn is the 100% owner of its subsidiaries 21st Century Oncology, LLC, 21st Century Oncology Management Services, Inc., and 21st Century Oncology Services, LLC.

109. Defendant 21st Century Oncology of California, a Medical Corporation, is a California corporation with its principal place of business in Florida. Defendant 21st Century Oncology of California, a Medical Corporation, is an affiliated professional corporation/association of 21st Century Oncology, Inc., which in turn is a subsidiary that is 100% owned by 21st Century Oncology Investments, LLC.

110. 21st Century Oncology Investments, LLC and 21st Century Oncology of California, a Medical Corporation (collectively "Defendants" or "21st Century") comprise a global, physician-led provider of integrated cancer care services, which bills itself as "the

premier provider of cancer care services across multiple modalities."[7] 21st Century claims to be the largest radiation oncology provider in the United States.

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

112. Defendants operate the largest integrated network of cancer treatment centers and affiliated physicians in the world. 21st Century operates in more than 500 locations in the United States, and employs or is affiliated with over 800 physicians, including medical oncologists, radiation oncologists, and other specialists that include urologists, hematologists, gynecologic oncologists, surgeons, and pathologists. 21st Century advertises that it maintains specialties in a number of cancer-related treatments and surgeries, including those such as radiation oncology, breast cancer surgery, colorectal surgery, gynecological surgery, general surgery, urology, pulmonology, and primary care, among others.

113. Defendants' cancer treatment centers in the United States are operated predominantly under the *21st Century Oncology* brand and are located 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. 21st Century also manages 36 treatment centers in seven countries in Latin America.

---

[7] 21st Century Oncology, *Corporate Overview*, https://www.21co.com/overview (last visited July 29, 2018).

V. FACTUAL ALLEGATIONS

A. 21st Century Released and Disclosed 21st Century Patient PII/PHI to One or More Unauthorized Parties, Who Offered the Data for Sale on the Dark Web

114. On or about November 6, 2015, the FBI learned that "an unauthorized party was attempting to sell compromised 21st Century Oncology data," which "was advertised, in Russian, as approximately 10 million patient records from 21st Century Oncology available to purchase for $10,000."[8] The FBI obtained a sample of the data from the unauthorized party.[9]

115. Around this time, the business risk intelligence company Flashpoint independently discovered the Data Breach "as part of [its] ongoing research concerning the theft of data and fraud that increasingly targets healthcare providers and insurers," and "[a]fter communicating with a threat actor who admitted that he had obtained records from 21st Century Oncology, Flashpoint sources contacted federal law enforcement."[10]

116. Pursuant to a request for information by Kroll, Flashpoint provided additional information regarding the unauthorized party who perpetrated the Data Breach, including that this individual's native language is Russian, and that this individual "indicated that the database was downloaded from 21st Century Oncology sometime between October 26, 2015 and November 1, 2015, and that it consisted of approximately 10 million records."[11] Further,

---

[8] FBI, Declaration of Special Agent Joseph Battaglia (June 5, 2018) ("FBI Decl.") ¶ 3.
[9] *Id.*
[10] Flashpoint, *21st Century Oncology Announces Data Breach Uncovered by Flashpoint*, at K00000761 (Mar. 8, 2016).
[11] Flashpoint, *Request for Information: 21st Century Oncology Compromise*, at KL00029098 (Mar. 10, 2016).

"[b]ased on circumstantial evidence obtained through the actor's forum activity, in particular his involvement with botnets," Flashpoint "estimate[d] that the information used to gain access to the network was gathered from botnet logs."[12]

117. Flashpoint also provided a sample of 21st Century patient data to Kroll.[13] Based on information and belief, Flashpoint received a separate and distinct sample of the patient data from the unauthorized party than what was provided to the FBI.

118. On November 13, 2015, and again on December 13, 2015, the FBI notified 21st Century "that patient information was illegally obtained by an unauthorized third party," and provided 21st Century a sample of the data obtained from the unauthorized party, consisting of certain "patient files purchased by an FBI informant."[14]

119. On November 19, 2015, 21st Century "confirmed that the sample of data provided by the FBI contained its patients' information," and the FBI informed 21st Century "that the unauthorized party listed additional data beyond the sample for sale."[15]

120. [redacted]

[12] *Id.*
[13] *Id.* at 4.
[14] Resolution Agreement and Corrective Action Plan between U.S. Department of Health and Human Services, Office for Civil Rights and 21st Century Oncology, Inc. ("OCR Settlement") at 1, https://www.hhs.gov/sites/default/files/21co-ra_cap.pdf; *see also Letter from 21st Century to Office of the Attorney General of New Hampshire* (Mar. 4, 2016) (hereinafter "NH Notification Letter"), http://doj.nh.gov/consumer/security-breaches/documents/21st-century-oncology-20160304.pdf (the FBI advised 21st Century that "patient information was illegally obtained by a third party who may have gained access to a 21st Century database"); FBI Decl., *supra* note 8, ¶ 4.
[15] FBI Decl., *supra* note 8, ¶ 6.
[16] Kroll, *Investigative Analysis Report for 21st Century Oncology, Inc.*, at 21C0000001, 21C0000005 (Apr. 17, 2016) (hereinafter "Investigative Report"); OCR Settlement, *supra* note 14, at 1.

121. [redacted]

122. [redacted]

123. [redacted]

[17] Letter from Lynn Sessions, Baker Hostetler, to Beatriz Romero-Escobar, U.S. Dept. of Health & Human Services, at 21C0004556 (Feb. 22, 2017).
[18] *Id.*
[19] *Id.*
[20] *See* OCR Settlement at 1, *supra* note 14, at 21C0008384 (June 23, 2017).

[redacted]

124. Further, 21st Century determined that, as a result of the Data Breach, "2,213,597 individuals were affected by the impermissible access to their names, social security numbers, physicians' names, diagnoses, treatment and insurance information."[23]

125. The Data Breach was the result of a persistent cyberattack that was ongoing for many months, was identified by the FBI, and was caused by 21st Century's failure to implement and maintain standard security procedures, such as adequate risk analysis and risk management, as well as failing to regularly review records of information systems activity, which would have immediately alerted 21st Century to the Data Breach.

126. [redacted]

[21] Letter from Lynn Sessions, Baker Hostetler, to Beatriz Romero-Escobar, U.S. Dept. of Health & Human Services, at 21C0008385 (June 23, 2017).
[22] *See* OCR Settlement, *supra* note 14, at 1-2.
[23] *Id.* at 1.
[24] Deposition of 30(b)(6) Witness – Benedetto Demonte (July 13. 2018) ("Demonte Depo.") at 232:1-20.

[redacted]

B. The Department of Health and Human Services Found 21st Century Impermissibly Disclosed the PII/PHI of More than 2.2 Million Patients

127. On December 28, 2017, the U.S. Department of Health and Human Services, Office for Civil Rights ("HHS") announced that it had entered into a Resolution Agreement and Corrective Action Plan ("OCR Settlement") with 21st Century.[26]

128. Regarding the scope of the Data Breach, HHS, which enforces regulatory standards including those that govern the privacy of individually identifiable health information, investigated the Data Breach and concluded that 21st Century ***"impermissibly disclosed the PHI of 2,213,597 of its patients."***[27]

129. HSS also concluded that:

- 21st Century "failed to conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of the electronic protected health information" held by 21st Century;
- 21st Century "failed to implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level";
- 21st Century "failed to implement procedures to regularly review records of

[25] *Id.* at 236:5-237:17.
[26] Press Release, U.S. Department of Health and Human Services, Office for Civil Rights, Failure to protect the health records of millions of persons costs entity millions of dollars (Dec. 28, 2017), https://www.hhs.gov/about/news/2017/12/28/failure-to-protect-the-health-records-of-millions-of-persons-costs-entity-millions-of-dollars.html.
[27] OCR Settlement, *supra* note 14, at 1 (emphasis added).

information system activity, such as audit logs, access reports, and security incident tracking reports"; and

- 21st Century "disclosed protected health information to [] third party vendors, acting as its business associates, without obtaining satisfactory assurances in the form of a written business associate agreement."[28]

130. These findings by the OCR indicate that 21st Century was negligent in securing its patients' PII/PHI and was directly responsible for impermissibly releasing, disclosing, and publishing the PII/PHI of more than 2.2 million of its patients.[29]

131. As part of the OCR Settlement, 21st Century agreed to pay $2.3 million to HHS for its conduct that resulted in the Data Breach.[30]

132. 21st Century also agreed to enter into a Corrective Action Plan, which obligates 21st Century to take specific corrective measures to address its actions and omissions that resulted in the Data Breach.[31]

C. [redacted]

133. [redacted]

[28] *Id.* 1-2.
[29] *Id.*
[30] *Id.* at 2.
[31] *Id.*
[32] Investigative Report, *supra* note 16, at 21C0000005.

134. [redacted]

135. [redacted]

136. [redacted]

137. [redacted]

[33] *Id.* at 21C0000005, 21C0000009.
[34] *Id.* at 21C0000005.
[35] *Id.* at 21C0000005, 21C0000009.

[redacted]

138. [redacted]

[redacted]

139. [redacted]

[redacted]

140. [redacted]

[redacted]

[36] *Id.* at 21C0000005, 21C0000010.
[37] *Id.* at 21C0000010.
[38] README.txt at 21C0001021.
[39] *Id.*
[40] *See* Investigative Report, *supra* note 16, at 21C0000009-11.

141. [redacted]

D. [redacted]

142. [redacted]

[41] *See id.*
[42] *Id.* at 21C0000007.
[43] *Id.* at 21C0000012.

[redacted]

[44] [redacted] *See id.* at 21C0000023.
[45] [redacted] *See id.* at 21C0000013.
[46] *Id.* at 21C0000012-13.
[47] *Id.* at 21C0000012.
[48] *Id.*
[49] *Id.* at 21C0000014.

[redacted]

143. [redacted]

144. [redacted]

[50] *Id.* at 21C0000013-14.
[51] *Id.*
[52] *Id.* at 21C0000016.
[53] *Id.*
[54] *Id.* at 21C0000006.
[55] *Id.* at 21C0000017; *see also* Demonte Depo., *supra* note 8, at 196:21-197:13 [redacted]

145. [redacted]

[56] Investigative Report, *supra* note 16, at 21C0000014; *see also* README.txt, *supra* note 38, at 21C0001021.
[57] *See* Investigative Report, *supra* note 16, at 21C0000005-06. [redacted]
[58] *See id.* at 21C0000006.

[redacted]

E. 21st Century's Acts and Omissions Contributed to the Release, Disclosure, and Publication of its Patients' PII/PHI

146. For at least three years prior to the Data Breach, 21st Century was aware that its inadequate data security made its patients' information highly vulnerable to compromise, rendering its PII/PHI publicly accessible to unauthorized parties.

147. [redacted]

[59] *See id.* at 21C0000005-06.
[60] Deloitte, *Information Technology Controls Audits*, at 21C0003589, 21C0003601 (2012-2015).
[61] *Id.* at 21C0003598-99, 21C0003601-02.
[62] *Id.* at 21C00035890-92, 21C0003602.

[redacted]

148. [redacted]

[redacted]

149. [redacted]

[redacted]

[63] *Id.* at 21C0003598.
[64] *Id.* at 21C0003603, 21C0003607.
[65] *Id.* at 21C0003601.
[66] CenturyLink, *Healthcare IT Security and Risk Assessment*, at 21C0003813-14.

[redacted]

150. [redacted]

[67] *See, e.g.*, CAaNES, *21st Century Oncology Internal Network Security Posture Assessment Report*, at 21C0008212 (Nov. 26, 2014).
[68] *Id.* at 21C0008207, 21C0008261.
[69] CAaNES, *Internal Network Security Posture Assessment Report*, at 21C0008220-21 (Nov. 26, 2014).
[70] *Id.*

[redacted]

[71] *Id.*
[72] *Id.*
[73] *Id.*
[74] *Id.*
[75] *Id.* at 21C0008222-23.
[76] CAaNES, *Internal Network Security Posture Assessment Report*, at 21C0008120 (Nov. 26, 2014).

151. [redacted]

[77] *Id.* at 21C0008122, 21C0008141-44.
[78] CAaNES, *External Network Security Posture Assessment Report* at 21C0008073 (Nov. 26, 2014).
[79] *Id.* at 21C0008074.
[80] CAaNES, *External Network Security Posture Assessment Report* at 21C0008026 (Nov. 26, 2014).
[81] CAaNES, *Web Application Security Assessment Developer Report* at 21C0007988 (Nov. 5, 2014).

- [redacted]

152. Based on information and belief, 21st Century's lack of reasonable care or concern in addressing these and other known vulnerabilities resulted in Plaintiffs' and Class members' PII/PHI being made publicly accessible to unauthorized parties through the internet, with no security, safeguards, or other protection whatsoever.

153. Because of these and other security audits and reports—including the CenturyLink report, the CAaNES reports, and Deloitte audits—21st Century undeniably knew that, by placing its patients' PII/PHI on its network, it was releasing, disclosing, and making its patients' information publicly accessible to unauthorized parties who could readily access its network.

F. [redacted]

154. [redacted]

155. [redacted]

156. [redacted]

157. [redacted]

[82] Letter from Baker Hostetler to HHS, *supra* note 17, at 21C0004553 (Feb. 22, 2017); Demonte Depo., *supra* note 24, at 38:20-39:7, 49:8-19, 50:11-13.
[83] Demonte Depo., *supra* note 8, at 63:17-64:2.

[redacted]

158. [redacted]

159. [redacted]

160. [redacted]

---

[84] Investigative Report, *supra* note 16, at 21C0000018-22.
[85] *Id.* at 21C0000021-22.
[86] *Id.* at 21C0000023.
[87] *Id.*

[redacted]

G. The Notification Provided by 21st Century to Plaintiffs and Class Members Was Delayed, Confusing, and Misleading

1. 21st Century's Delayed Disclosure of the Data Breach Further Harmed Plaintiffs and Class Members

161. Despite the risk to its patients of fraud and other identity theft, 21st Century delayed notifying patients of the Data Breach until March 4, 2016, almost four months after it was informed of the Data Breach.[90]

162. In the intervening months between when the FBI notified 21st Century of the Data Breach and when 21st Century disclosed it to Plaintiffs and Class members, 21st Century focused ***not*** on protecting patients and others whose PII/PHI it released, disclosed, and made publicly accessible through its lax security measures, but rather on controlling the damage to itself and its investors.

163. During the four months during which 21st Century failed to notify Plaintiffs and Class members of the Data Breach, Plaintiffs and Class members were at an especially

---

[88] *Id.*
[89] *Id.*
[90] *See* NH Notification Letter, *supra* note 14.

heightened risk of identity theft. Not only was their most sensitive PII/PHI already for sale on the internet without their knowledge, but this period overlapped with months during which income tax returns are filed, putting them at an increased risk of tax fraud.

164. For this reason, many Class members were blindsided by the notification that their Social Security numbers had been compromised, with only weeks remaining before the tax-filing deadline. Further, many Class members found activating the credit monitoring service to be confusing and time consuming, thereby increasing the stress and anxiety associated with uncertainty about whether the Data Breach would jeopardize any expected tax refunds.

2. 21st Century's Notification Was False and/or Misleading and Obscured Key Facts About the Data Breach

165. Despite having had months to prepare its notification to Plaintiffs and Class members, the March 4, 2016 notification letter sent by 21st Century indicates only that, "on October 3, 2015, [an] intruder ***may*** have accessed [a] database, which contained information that ***may*** have included your name, Social Security number, physician's name, diagnosis and treatment information, and insurance information"[91] Further, 21st Century represented to Plaintiffs and Class members that "[w]e have no evidence that your medical record was accessed," and "[w]e have no indication that your information has been misused in any way."[92]

166. As is indicated above, this notification was false and/or misled Plaintiffs and

[91] *Id.* (emphases added).
[92] *Id.*

Class members by inaccurately conveying that 21st Century did not possess information that patient medical information had, in fact, been improperly released, disclosed, and published to unauthorized parties. At that time, however, Defendants were fully aware not only that patient medical information had been obtained by unauthorized parties, but that such information was being offered for sale on the internet as early as November 2015. Moreover, 21st Century's notification concealed the fact that—due to 21st Century's inadequate and insufficient data security and information retention policies and practices—Defendants never adequately investigated or attempted to ascertain which of their patients' medical information had been disclosed to unauthorized parties or offered for sale on the internet.

167. In this regard, the notification letter that 21st Century ultimately mailed to Plaintiffs and Class members failed to provide concrete information about the Data Breach and incompletely described what PII/PHI was in fact exposed, how it was exposed, and what changes 21st Century was making to prevent further compromises of PII/PHI in the future.

3. 21st Century's Notification Was Confusing to Plaintiffs and Class Members

168. When Plaintiffs and Class members began receiving the notification letters from 21st Century on or about March 12, 2016, some of them did not understand that they had a relationship with 21st Century, because 21st Century operates numerous facilities throughout the country under different trade names. For this reason, some Plaintiffs and Class members believed the notification letters they received from 21st Century to be a scam.

169. Indeed, as of March 18, 2016, it was not obvious to Plaintiffs and Class members looking to confirm the authenticity of the notification letter through 21st Century's website that there had been a Data Breach. While a single line, "A Message to Our Patients

Regarding Security Incident" appears in small font on the home page of 21st Century's website; it did not prominently appear at the top or bottom of the screen and was masked amongst other text and images on the elongated home page.

170. For this reason, many recipients of 21st Century's notification letters discarded the letters and did not take action to obtain the credit monitoring services offered by 21st Century during the short four-month window that 21st Century allowed Plaintiffs and Class members to sign up for the offered services.

171. Other Data Breach victims who were unfamiliar with the name "21st Century Oncology" were left to play detective to ascertain which physicians they had seen were associated with 21st Century.

4. Industry Insiders Confirm That 21st Century's Data Breach Notification Was Insufficient and Inadequate

172. Ted Harrington, executive partner with Independent Security Evaluators, a

security assessment and consulting firm, expressed the opinion that 21st Century's notification was inadequate and misleading:

> 21st Century Oncology's response really misses the mark. They note in their statement that no medical records were lost. But patient names, Social Security numbers and other data were. These are some of the most important aspects of the medical record.[93]

173. For the foregoing reasons, 21st Century's delayed and inadequate notification of the Data Breach resulted in additional damage and created additional hardships for Plaintiffs and Class members who were already experiencing medical and financial difficulties.

H. 21st Century Acknowledged Its Duty to Keep PII/PHI Private

174. 21st Century routinely requests, records, collects and/or generates protected PII/PHI about its patients that includes, but is not limited to, patient names, Social Security numbers, physicians' names, diagnoses and treatment information, and insurance information.

175. 21st Century owed a common law duty to Plaintiffs and Class members to protect PII/PHI entrusted to it, including to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, protecting, and preventing the PII/PHI in its possession from being impermissibly released, disclosed, published, compromised, stolen, accessed, and misused by unauthorized parties.

176. 21st Century further owed and breached its duty to Plaintiffs and the Class to

---

[93] Paul Benjou, *Negligence is the Cancer of CyberCrime* (Mar. 2016), http://myopenkimono.blogspot.com/search?q=negligence+is+the+cancer.html (last visited July 26, 2018).

implement processes and specifications that would detect a breach of its security systems in a timely manner and to timely act upon warnings and alerts, including those generated by its own security systems.

1. Industry Standards Also Provide Guidelines to Healthcare Providers Regarding Best Practices for Securing Confidential Medical Information

177. 21st Century owed and breached its duties to Plaintiffs and Class members to provide and maintain reasonable security over PII/PHI security consistent with industry standards including, but not limited to, Cloud Security Alliance (CSA) Cloud Controls Matrix, CMS Information Security ARS 2010, COBIT 4.1 and 5, Iso/IEX 27001:2005, ISO/IEX 27002:2005; ISO/IEC 27799:2008, and Joint Commission (formerly the Joint Commission on the Accreditation of Healthcare Organizations, JCAHO). Likewise, 21st Century owed a duty and breached its duties to Plaintiffs and Class members to design, maintain, and test its security systems and networks to ensure that PII/PHI in 21st Century's possession was adequately secured and protected.

I. 21st Century Was Aware of the Risk of Data Breach and the Value of the PII/PHI with Which It Was Entrusted

1. From 2011 To 2012, 21st Century Experienced a Data Breach Involving Patient PII/PHI

178. 21st Century is no stranger to data breaches. On or about May 15, 2013, federal law enforcement officials informed 21st Century that one of its employees had improperly disclosed patient PII/PHI over the course of almost ten months between October 11, 2011 and August 8, 2012 (the "2011-2012 Data Breach"). The 21st Century employee disclosed patient PII/PHI to a third party who used patient names, Social Security numbers, and dates of birth to file fraudulent claims for tax refunds. As with the recently announced

Data Breach, 21st Century failed to both prevent and to detect the 2011-2012 Data Breach.

179. When 21st Century notified the Maryland Attorney General of the 2011-2012 Data Breach on or about July 10, 2013, 21st Century had not yet concluded its own internal investigation into how the employee was able to access this information.

180. Ultimately, 21st Century 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 21st Century . . . and we take any potential misuse of our patients' private health information very seriously." [94]

181. In the ensuing years, however, 21st Century did not carry through with its assurances and only obtained—and thereby put at risk—far more patient data.

2. The FBI Made a Highly Publicized Warning to Healthcare Companies such as 21st Century about the Increased Risk of Cyber Attacks

182. According to cybersecurity company SANS Institute, healthcare providers and health insurance companies are regular targets of cyber-attacks, and were particularly vulnerable to them by October 2013.[95]

183. In April 2014, the FBI's cyber division warned healthcare systems that cyber-attacks were likely to further increase after January 2015, when healthcare companies were required to switch from using paper medical records to electronic records. The FBI noted that

---

[94] Letter from 21st Century to Office of the Attorney General of Maryland (Jul. 10, 2013).

[95] 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 (last visited July 26, 2018).

healthcare companies were more susceptible to cyber-attacks, making future attacks likely.[96]

184. The FBI's report was highly publicized in 2014, being reported by such news agencies as Reuters.[97]

185. However, 21st Century did not heed these warnings to reasonably and adequately secure this private and highly sensitive PII/PHI, as demonstrated by its failure to learn of the recently disclosed Data Breach until the FBI (again) reported it to 21st Century.

186. 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[.][98]

J. 21st Century Has a Marked History of Prioritizing Profit Over Patients, Including Engaging in Fraudulent Billing Practices and Performing Unnecessary Tests on its Patients for at least Seven Years

187. The Data Breach must be viewed in the context of the 21st Century corporate culture in which it arose. Contrary to its stated commitment to provide "compassionate" cancer care to patients,[99] 21st Century, through its wholly-owned subsidiaries, has been subjecting patients to a variety of unnecessary medical testing for years.

---

[96] Federal Bureau of Investigation, *FBI Cyber Division Private Industry Notification* (Apr. 8, 2014), https://info.publicintelligence.net/FBI-HealthCareCyberIntrusions.pdf (last visited July 26, 2018).
[97] Finkle, *Exclusive: FBI Warns Healthcare Sector Vulnerable to Cyber Attacks*, Reuters (Apr. 23, 2014), http://www.reuters.com/article/2014/04/23/us-cybersecurity-healthcare-fbi-exclusividUSBREA3M1Q920140423 (last visited July 26, 2018).
[98] 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 (last visited July 26, 2018).
[99] 21st Century Oncology, *Home Page*, https://www.21co.com (last visited July 26, 2018).

188. On March 25, 2013—two months before the FBI informed 21st Century of the 2011-2012 Data Breach—a medical assistant filed a whistleblower suit against a 21st Century subsidiary alleging a scheme to subject patients to unnecessary tests in order to fraudulently collect money from federal healthcare programs from 2008 through 2012.[100]

189. 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."[101]

190. On December 16, 2015—one month after the FBI informed 21st Century of the recently disclosed Data Breach—21st Century filed an SEC Form 8-K that announced that it was settling the whistleblower suit for $19.75 million.[102]

191. On October 19, 2015—less than a month before the FBI informed 21st Century of the instant Data Breach—a doctor filed a whistleblower suit against a 21st

---

[100] *United States, State of Fl., ex rel. Barnes v. Spellberg, 21st Century and Naples Urology Assoc.*, No. 2:13-cv-228-FtM-99DNF (M.D. Fla.).
[101] 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 (last visited July 26, 2018).
[102] 21st Century Oncology, SEC Form 8-K (Dec. 16, 2015).

Century subsidiary alleging a scheme to subject patients to four categories of unnecessary tests in order to fraudulently collect money from federal healthcare programs from 2009 through 2014.[103]

192. In this case, "[t]he company prioritized profit over medical counsel," said David L. Scher, counsel for the whistleblowing doctor.[104]

193. 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."[105]

194. On March 9, 2016—days after publicly disclosing the Data Breach—21st Century filed an SEC Form 8-K announcing that it was settling the second whistleblower suit for $34.7 million.[106]

K. 21st Century's Response to the Data Breach Is Inadequate and Is Insufficient to Address the Ongoing Risks and Harms to Plaintiffs and Class Members

1. The Risk of Identity Theft Is a Major Concern to Plaintiffs and Class Members

195. There is a strong likelihood that Plaintiffs and Class members are already or

---

[103] *United States ex rel. Ting v. 21st Century Oncology and So. Fl. Radiation Oncology*, No. 3:14-cv-723-Jax-J32JRK (M.D. Fla).

[104] 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 (last visited July 26, 2018).

[105] *Id.*

[106] 21st Century Oncology, SEC Form 8-K (Mar. 9, 2016).

will become victims of identity theft and fraud, given the breadth of PII/PHI about them that has been released, disclosed, and published.

196. The likelihood of such identity theft and fraud is significantly increased by the fact that Plaintiffs and Class members' PII/PHI has already been publicly offered for sale to identity thieves on the internet, as the FBI informed 21st Century in November 2015.

197. 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.[107]

198. Hackers steal such PII/PHI in order to sell it on black market sites to identity thieves,[108] who attempt to get their money's worth from such information by committing identity theft and fraud.

199. The likelihood or probability that Plaintiffs' and Class members' PII/PHI would be improperly used, sold, or otherwise mishandled led 21st Century to offer one year of credit monitoring and identity-theft protection to the approximately 2.2 million people whom it determined were affected by the Data Breach, after the FBI informed it that patient information was illegally obtained by a third party in October 2015.

200. It costs 21st Century more than a *de minimis* amount to provide these services

---

[107] Javelin Strategy, *2014 Identity Fraud Report: Card Data Breaches and Inadequate Consumer Password Habits Fuel Disturbing Fraud Trends* (Feb. 5, 2014), https://www.javelinstrategy.com/coverage-area/2014-identity-fraud-report-card-data-breaches-and-inadequate-consumer-password-habits (last visited July 29, 2018).

[108] Ozzie Fonseca, *Following Personal Identifying Information (PII/PHI) Down the Black Net Road*, Experian (Aug. 11, 2015), http://www.experian.com/blogs/data-breach/2015/08/11/following-personal-identifying-information-PII/PHI-down-the-black-net-road/ (last visited July 26, 2018).

to the 2.2 million Data Breach victims. Experian currently charges between $9.99 and $19.99 per month for its identity theft protection services for individuals.[109] 21st Century has offered these services to Plaintiffs and Class members because the risk of identity theft to Plaintiffs and Class members cannot be safely disregarded.

2. Compromised Social Security Numbers Have Long-Term Value to Thieves and Long-Term Consequences to Data Breach Victims

201. 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."[110]

202. Unfortunately, Plaintiffs and Class members have to wait until they become victims of Social Security number misuse before they can obtain a new one.

203. Even then, the Social Security Administration warns "that a new number probably won't solve all [] problems . . . and won't guarantee . . . a fresh start." In fact, "[f]or some victims of identity theft, a new number actually creates new problems."[111] 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.

3. Compromised Medical Information Has Even Greater Long-Term Value to Identity Thieves and Consequences for Plaintiffs and Class Members

204. Kunal Rupani, director of product management at Accellion, a private cloud

---

[109] Experian, *Identity Theft Protection*, http://www.experian.com/consumer-products/identity-theft-and-credit-protection.html (lasted visited July 29, 2018).
[110] Cameron Huddleston, *How to Protect Your Kids From the Anthem Data Breach*, Kiplinger, (Feb. 10, 2015), http://www.kiplinger.com/article/credit/T048-C011-S001-how-to-protect-your-kids-from-the-anthem-data-brea.html# (last visited July 29, 2018).
[111] Social Security Admin., *Identity Theft and Your Social Security Number*, at 6-7, https://www.ssa.gov/pubs/EN-05-10064.pdf (last visited July 26, 2018).

solutions company, told *eSecurity Planet* that it's likely the 21st Century hackers were targeting the Data Breach victims' PII/PHI for its long-term value, stating:

> Unlike credit card numbers and other financial data, healthcare information doesn't have an expiration date. 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.[112]

205. PII/PHI—like the type disclosed in the breach—is particularly valuable for cybercriminals. According to SecureWorks (a division of Dell Inc.), "[i]t's a well known truism within much of the healthcare data security community that an individual healthcare record is worth more on the black market ($50, on average) than a U.S.-based credit card and personal identity with social security number combined."[113] The reason is that thieves "[c]an use a healthcare record to submit false medical claims (and thus obtain free medical care), purchase prescription medication, or resell the record on the black market."[114]

206. Similarly, the FBI Cyber Division, in an April 8, 2014 Private Industry Notification, advised:

> Cyber criminals are selling [medical] information on the black market at a rate of $50 for each partial EHR, compared to $1 for a stolen social security number or credit card number. EHR can then be used to file fraudulent insurance claims, obtain prescription medication, and advance identity theft. EHR theft is also more difficult to detect, taking almost twice as long as normal identity theft.[115]

---

[112] *See* Goldman, *supra* note 98.
[113] *What's the Market Value of a Healthcare Record*, Dell SecureWorks (Dec. 13, 2012), https://www.secureworks.com/blog/general-market-value-of-a-healthcare-record (last visited July 26, 2018).
[114] *Id.*
[115] *FBI Cyber Division Private Industry Notification*, *supra* note 96.

4. Thieves Will Likely Use Plaintiffs' and Class Members' PII/PHI to Hurt Them Far Longer Than One Year

207. Once hackers have such PII/PHI, "they can use it to procure prescription drugs or expensive medical equipment or simply to commit financial fraud—often for months or years before anyone notices."[116]

208. 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 monetize victims' identifies over a longer period of time."[117] 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. [118]

209. This truth is notably acknowledged in the ProtectMyID attachment to 21st Century's notification letter to Plaintiffs and Class members, which states that "[i]t is recognized that identity theft can happen months and even years after a data breach."[119]

5. The Consequences to Victims of Medical Identity Theft Can Be Time Consuming, Financially Devastating, and Even Life Threatening

210. Once use of compromised non-financial PII/PHI is detected, the personal and economic consequences to the data breach victims can be overwhelming. As reported by CreditCards.com:

---

[116] Cathleen McCarthy, CreditCards, *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 (last visited July 29, 2018).
[117] *Id.*
[118] *See* Goldman, *supra* note 98.
[119] *See* NH Notification Letter, s*upra* note 14.

> 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.[120]

211. Research by Ponemon confirms that medical identity theft is costly and complex to resolve, and therefore it is critical for healthcare providers to take additional steps to assist victims resolve the consequences of the theft and prevent future fraud. In a 2014 study, Ponemon found that sixty-five percent (65%) of victims of medical identity theft in the study had to pay an average of $13,500 to resolve the resultant crimes[121], and only ten percent (10%) of those in the study reported having achieved complete satisfaction in concluding the incident.

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

---

[120] McCarthy, *supra* note 116.

[121] Jaclyn Fitzgerald, *Ponemon Institute Study Reveals 21.7% Rise in Medical Identity Theft,* HC Pro (Mar. 2, 2015), http://www.hcpro.com/HIM-313785-865/Ponemon-Institute-study-reveals-217-rise-in-medical-identity-theft.html (last visited July 26, 2018).

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

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

214. The injuries suffered and likely to be suffered by Plaintiffs and Class members are and will be a direct and proximate result of the Data Breach, including:

(a) release, disclosure, and publication of their personal and financial information;

(b) loss or delay of tax refunds as a result of fraudulently filed tax returns;

(c) costs associated with the detection and prevention of identity theft and unauthorized use of their PII/PHI with regard to financial, business, banking, and other accounts;

(d) costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and

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

(e) the imminent and certain impending injury flowing from fraud and identity theft posed by their PII/PHI being placed in the hands of hackers and being offered for sale on the Dark Web;

(f) damages to and diminution in value of their PII/PHI entrusted to 21st Century for the sole purpose of obtaining healthcare services from 21st Century;

(g) money paid to 21st Century for healthcare services during the period of the Data Breach, because Plaintiffs and Class members would not have obtained healthcare services from 21st Century had it disclosed that it lacked adequate systems and procedures to reasonably safeguard patients' PII/PHI;

(h) overpayments to 21st Century for healthcare services purchased, in that a portion of the amount paid by Plaintiffs and Class members to 21st Century was for the costs for 21st Century to take reasonable and adequate security measures to protect the Plaintiffs and Class members' PII/PHI, which 21st Century failed to do; and

(i) personal, professional, or financial harms caused as a result of having their PII/PHI exposed.

215. 21st Century and their agents have received numerous complaints of identity theft from Class members who allege their information has been used fraudulently and without their permission.

216. 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 even be life-threatening:

> The extreme circumstances, [medical identity theft] could be life-threatening if the wrong information ends up in your medical record.[122]

For instance, if incorrect medical information such as blood type or allergies becomes commingled in a data breach victim's medical records, that misinformation can be deadly if that individual becomes unconscious and needs an emergency transfusion or injection.[123]

6. Many of the Affected Patients Comprise a Vulnerable Population

217. Undergoing treatment for cancer often demands significant amounts of time and energy, and can cause painful side effects. Many cancer patients are unable to monitor their financial accounts and credit reports with the same diligence as healthy individuals. The nature of their diagnosis and treatment renders cancer patients, as a group, more vulnerable to financial fraud and identity theft than healthy individuals.

218. In this regard, James Chappell, Digital Shadows' CTO and co-founder, expressed surprise at 21st Century's failure to protect the PII/PHI of its patients, particularly

---

[122] Office of Inspector General, *Medical Identity Theft & Medicare Fraud Brochure*, at 1, https://oig.hhs.gov/fraud/medical-id-theft/OIG_Med_Id_Theft_Brochure.pdf (last accessed July 29, 2018).
[123] McCarthy, *supra* note 116.

given their known life circumstances, stating:

> The circumstances in these patients' lives were already pretty tough . . . I'm surprised 21st Century Oncology weren't better stewards of their patients' data given their circumstances.[124]

219. Further, cancer disproportionately affects the elderly. Senior citizens are targeted for financial fraud and identity theft at higher rates than non-senior citizens. Identity theft and financial exploitation are among the most commonly reported forms of fraud perpetrated against the elderly.

7. The Remedy Offered By 21st Century Is Inadequate, and Requires Plaintiffs and Class Members to Expend Time on an Ongoing Basis to Contain Their Compromised PII/PHI

220. 21st Century previously offered Plaintiffs and Class members twelve months of credit monitoring and identity theft insurance with ProtectMyID, an Experian product. However, this now unavailable remedy does not fully protect Plaintiffs and Class members against the risk of identity theft and fraud. Further, the twelve-month coverage period provided is insufficient to protect Plaintiffs and Class members, as it is far shorter than the period that they are likely to become victims of identity theft and fraud.

221. 21st Century sent out letters on March 4, 2016 to Plaintiffs and Class members, offering them twelve months of credit monitoring. However, Defendants provided only a very short window of time in which to accept this offer. Plaintiffs and Class members were given only until July 7, 2016—fewer than four months—to receive the letter, learn their

[124] 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 visited July 26, 2018).

options, and decide whether to accept the monitoring. Plaintiffs and Class members who tried enrolling after that date were denied enrollment. This unrealistic deadline posed a problem for Plaintiffs and Class members who initially believed the letter itself was a scam; who did not receive their letter immediately to their current address; who were undergoing treatment and were not able to respond in the short time window; and/or for those who were still researching their options. Here, again, 21st Century placed its financial position before the well-being of its patients.

222. In any event, the previously offered credit monitoring and identity theft insurance cannot fully protect Plaintiffs and Class members against identity theft or fraud. In this regard, credit monitoring is reactionary and only detects activity ***after*** identity thieves use compromised PII/PHI to attempt to fraudulently open lines of credit. Similarly, identity theft insurance only reimburses losses ***after*** they have occurred.

223. Accordingly, 21st Century recommended that Plaintiffs and Class members monitor their explanation of benefits statements to detect and resolve unauthorized charges without its help. The notification letter sent by 21st Century to Plaintiffs and Class members stated:

> 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.[125]

224. Further, among the recommendations in the ProtectMyID attachment to 21st Century's Data Breach notification letter to Plaintiffs and Class members was that Data

[125] *See* NH Notification Letter, *supra* note 14 (emphases added).

Breach victims take the following steps on their own: (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" for those who believe that they have become "a victim of identity theft or have reason to believe [their] personal information has been misused."[126]

225. These tasks are significant burdens to ask of anyone who entrusted PII/PHI to another, and it is particularly reprehensible for 21st Century to shift its responsibility to its oncology patients and their loved ones.

226. In sum, the twelve months of credit monitoring and identity theft insurance offered by 21st Century does not in itself adequately protect Plaintiffs and Class members from a lifetime of identity theft risk and does nothing to reimburse Plaintiffs and Class members for the injuries they have already suffered.

VI. CLASS ACTION ALLEGATIONS

227. Plaintiffs bring claims pursuant to Federal Rule of Civil Procedure 23 on behalf of the following Nationwide Class, as defined below.

A. Nationwide Class

228. Plaintiffs bring their negligence, gross negligence, negligent misrepresentation, breach of express contracts, breach of implied contracts, breach of implied duty of good faith and fair dealing, breach of fiduciary duty, unjust enrichment, invasion of

[126] *Id.*

privacy, and declaratory judgment claims (Counts I-X) on behalf of a proposed nationwide Class ("Nationwide Class"), defined as follows:

> *All natural persons in the United States whose PII/PHI was compromised as a result of the Data Breach.*

229. Except where otherwise noted, "Class members" shall refer to members of the Nationwide Class.

230. Excluded from the Nationwide Class are Defendants and their current employees, as well as the Court and its personnel presiding over this action.

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

232. **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 21st Century had a legal duty to use reasonable security measures to protect Class members' PII/PHI from impermissible release, disclosure, and publication;

(b) Whether 21st Century timely, accurately, and adequately informed Class members that their PII/PHI had been compromised;

(c) Whether 21st Century breached its legal duty by failing to protect Class members' PII/PHI;

(d) Whether 21st Century acted reasonably in securing Class members' PII/PHI;

(e) Whether Class members are entitled to actual damages; and

(f) Whether Class members are entitled to injunctive relief.

233. **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 21st Century's uniform wrongful conduct and their legal claims all arise from the same conduct by 21st Century.

234. **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.

235. **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 21st Century'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.

236. **Rule 23(b)(2).** Plaintiffs also satisfy the requirements for maintaining a class action under Rule 23(b)(2). 21st Century 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.

237. **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
(On Behalf of the Nationwide Class)

238. Plaintiffs incorporate all foregoing factual allegations as if fully set forth herein.

239. 21st Century owed a duty to Plaintiffs and Class members, arising from the sensitivity of the information, the expectation that information was going to be kept private, and the foreseeability of its data security shortcomings resulting in an impermissible release, disclosure, and publication to unauthorized parties, to exercise reasonable care in safeguarding their sensitive personal information. This duty included, among other things, designing, implementing, maintaining, monitoring, and testing 21st Century's networks, systems, protocols, policies, procedures and practices to ensure that Plaintiffs' and Class members' information was adequately secured from impermissible release, disclosure, and publication.

240. 21st Century's Notice of Privacy Practices acknowledged 21st Century's duty to adequately protect Plaintiffs' and Class members' PII/PHI.

241. 21st Century owed a duty to Plaintiffs and Class members to implement administrative, physical, and technical safeguards, such as intrusion detection processes that detect data breaches in a timely manner, to protect and secure Plaintiffs' and Class members' PII/PHI from impermissible release, disclosure, and publication.

242. 21st Century also had a duty to only maintain PII/PHI that was needed to serve patient needs.

243. 21st Century owed a duty to disclose the material fact that its data security practices were inadequate to safeguard Plaintiffs' and Class members' PII/PHI.

244. 21st Century had a special relationship with Plaintiffs and Class members as a result of being entrusted with their PII/PHI, which provided an independent duty of care. Plaintiffs' and Class members' willingness to entrust 21st Century with their PII/PHI was predicated on the understanding that 21st Century would take adequate security precautions. Moreover, 21st Century was capable of protecting its networks and systems, and the PII/PHI it stored on them, from improper access, release, disclosure, and publication.

245. 21st Century breached its duties by, among other things: (a) failing to implement and maintain adequate data security practices to safeguard and prevent impermissible release, disclosure, and publication of Plaintiffs' and Class members' PII/PHI, including administrative, physical, and technical safeguards; (b) failing to detect the Data Breach in a timely manner; (c) failing to disclose that its data security practices were inadequate to safeguard and prevent impermissible release, disclosure, and publication of Plaintiffs' and Class members' PII/PHI; and (d) failing to provide adequate and timely notice of the Data Breach to Plaintiffs and Class members.

246. But for 21st Century's breach of its duties, including its duty to use reasonable care to protect and secure Plaintiffs' and Class members' PII/PHI, Plaintiffs' and Class members' PII/PHI would not have been impermissibly released, disclosed, and published.

247. Plaintiffs and Class members were foreseeable victims of 21st Century's inadequate data security practices. 21st Century knew or should have known that allowing its data security systems to be accessible to unauthorized parties would result in the impermissible release, disclosure, and publication of Plaintiffs' and Class members' PII/PHI and cause damage to Plaintiffs and Class members.

248. It was reasonably foreseeable that failing to implement and maintain reasonable data security practices and protocols would render its networks, databases, and computers that stored or contained Plaintiffs' and Class members' PII/PHI publicly accessible to unauthorized parties.

249. As a result of 21st Century's negligent failure to prevent the Data Breach, Plaintiffs and Class members suffered injury, which includes, but is not limited to, impermissible release, disclosure, and publication of their PII/PHI, both directly and indirectly by 21st Century as well as by unauthorized parties, and exposure to a heightened, imminent risk of fraud, identity theft, and financial harm. Plaintiffs and Class members must monitor their financial accounts and credit histories more closely and frequently to guard against identity theft. Plaintiffs and Class members also have incurred, and will continue to incur on an indefinite basis, out-of-pocket costs for obtaining credit reports, credit freezes, credit monitoring services, and other protective measures to deter and detect identity theft. The unauthorized release, disclosure, and publication of Plaintiffs' and Class members'

PII/PHI has also diminished the value of their PII/PHI.

250. The harm to Plaintiffs and Class members was a proximate, reasonably foreseeable result of 21st Century's breaches of its aforementioned duties.

251. Therefore, Plaintiffs and Class members are entitled to damages in an amount to be proven at trial.

COUNT II
GROSS NEGLIGENCE
(On Behalf of the Nationwide Class)

252. Plaintiffs incorporate all foregoing factual allegations as if fully set forth herein.

253. Plaintiffs and Class members entrusted 21st Century with highly-sensitive and inherently personal private data subject to confidentiality and physician-patient privileges.

254. In requiring, obtaining and storing Plaintiffs' and Class members' PII/PHI, 21st Century owed a duty of reasonable care in safeguarding this PII/PHI.

255. 21st Century's networks, systems, protocols, policies, procedures and practices, as described above, were not adequately designed, implemented, maintained, monitored and tested to ensure that Plaintiffs' and Class members' PII/PHI were secured from release, disclosure, and publication.

256. 21st Century's networks, systems, protocols, policies, procedures and practices, as described above, were not reasonable given the sensitivity of the Plaintiffs' and Class members' private data and the known vulnerabilities of 21st Century's systems.

257. Upon learning of the Data Breach, 21st Century should have immediately disclosed the Data Breach to Plaintiffs and Class members, credit reporting agencies, the

Internal Revenue Service, financial institutions, and all other third parties with a right to know and the ability to mitigate harm to Plaintiffs and Class members as a result of the Data Breach.

258. Despite knowing its networks, systems, protocols, policies, procedures and practices, as described above, were not adequately designed, implemented, maintained, monitored and tested to ensure that Plaintiffs' and Class members' PII/PHI were secured from release, disclosure, and publication, 21st Century ignored the inadequacies and was oblivious to the risk of release, disclosure, and publication it had created.

259. 21st Century's behavior establishes facts evidencing a reckless disregard for Plaintiffs' and Class members' rights.

260. 21st Century, therefore, was grossly negligent.

261. The negligence is directly linked to Plaintiffs' and Class members' injuries.

262. As a result of 21st Century's reckless disregard for Plaintiffs' and Class members' rights by failing to secure their PII/PHI despite knowing its networks, systems, protocols, policies, procedures, and practices were not adequately designed, implemented, maintained, monitored, and tested, Plaintiffs and Class members suffered injury, which includes, but is not limited to, impermissible release, disclosure, and publication—both directly and indirectly by 21st Century as well as unauthorized parties—of their PII/PHI as well as exposure to a heightened, imminent risk of fraud, identity theft, financial and other harm. Plaintiffs and Class members must monitor their financial accounts and credit histories more closely and frequently to guard against identity theft. Plaintiffs and Class members also have incurred, and will continue to incur on an indefinite basis, out-of-pocket costs for

obtaining credit reports, credit freezes, credit monitoring services, and other protective measures to deter or detect identity theft. The impermissible release, disclosure, and publication of Plaintiffs' and Class members' PII/PHI has also diminished the value of their PII/PHI.

263. The harm to Plaintiffs and the Class members was a proximate and reasonably foreseeable result of 21st Century's breach of its duty of reasonable care in safeguarding Class members' PII/PHI.

264. Therefore, Plaintiffs and Class members are entitled to damages in an amount to be proven at trial.

COUNT III
NEGLIGENT MISREPRESENTATION
(On Behalf of the Nationwide Class)

265. Plaintiffs incorporate all foregoing factual allegations as if fully set forth herein.

266. 21st Century negligently and recklessly misrepresented material facts pertaining to the provision of healthcare services to Plaintiffs and Class members by representing they would maintain adequate data privacy and security practices and procedures to safeguard Plaintiffs' and Class members' PII/PHI from impermissible release, disclosure, and publication.

267. Prior to making these representations, 21st Century knew its networks, systems, protocols, policies, procedures and practices, as described above, were not adequately designed, implemented, maintained, monitored and tested to ensure that Plaintiffs' and Class members' PII/PHI were adequately secured from release, disclosure,

and publication.

268. In reliance upon these representations, Plaintiffs and Class members engaged and paid for 21st Century to provide healthcare services to Plaintiffs and Class members.

269. Had Plaintiffs and Class members, as reasonable persons, known of 21st Century's inadequate data privacy and security practices, they would not have engaged 21st Century to provide, nor paid for, healthcare services from 21st Century, and would not have entrusted their PII/PHI to 21st Century.

270. As a direct and proximate consequence of 21st Century's negligent misrepresentations, Plaintiffs and Class members have suffered injury, which includes, but is not limited to, release, disclosure, and publication of their PII/PHI as well as exposure to a heightened, imminent risk of fraud, identity theft, financial and other harm. Plaintiffs and Class members must monitor their financial accounts and credit histories more closely and frequently to guard against identity theft. Plaintiffs and Class members also have incurred, and will continue to incur on an indefinite basis, out-of-pocket costs for obtaining credit reports, credit freezes, credit monitoring services, and other protective measures to deter or detect identity theft. The unauthorized release, disclosure, and publication of Plaintiffs' and Class members' PII/PHI has also diminished the value of the PII/PHI.

271. Therefore, Plaintiffs and Class members are entitled to damages in an amount to be proven at trial.

COUNT IV
BREACH OF EXPRESS CONTRACTS
(On Behalf of the Nationwide Class)

272. Plaintiffs reallege and incorporate by reference the allegations contained in

each of the preceding paragraphs as if fully set forth herein.

273. Plaintiffs and members of the Class, additionally and alternatively, allege that they entered into valid and enforceable express contracts, or were third party beneficiaries of valid and enforceable express contracts, with 21st Century.

274. Under these express contracts, 21st Century and/or its affiliated healthcare providers, promised and were obligated to: (a) provide healthcare to Plaintiffs and Class members; and (b) protect Plaintiffs' and the Class members' PII/PHI: (i) provided to obtain such healthcare; and/or (ii) created as a result of providing such healthcare. In exchange, Plaintiffs and members of the Class agreed to pay money for these services.

275. Both the provision of healthcare and the protection of Plaintiffs' and Class members' PII/PHI were material aspects of these contracts.

276. At all relevant times, 21st Century expressly represented that it is "required by law" to provide Plaintiffs and Class members with notice of 21st Century's "legal duties and privacy practices with respect to that health information." 21st Century's Notice of Privacy Practices that was published on 21st Century's website at all times relevant hereto, for example, expressly represented that 21st Century would "abide by the terms of the notice currently in effect," which included maintaining "the privacy of your protected health information" as required by law.[127] 21st Century also expressly represented in the Notice of Privacy Practices that it would notify any affected individuals following a breach of any unsecured protected health information.[128]

---

[127] *See* 21st Century, *Notice of Privacy Practices*, *supra* note 6.
[128] *Id.*

277. 21st Century's express representations, including, but not limited to, express representations found in 21st Century's Notice of Privacy Practices, formed an express contract requiring 21st Century to implement data security adequate to safeguard and protect the privacy of Plaintiffs' and Class members' PII/PHI.

278. Alternatively, the express contracts included implied terms requiring 21st Century to implement data security adequate to safeguard and protect the confidentiality of Plaintiffs' and Class members' PII/PHI, including in accordance with industry standards.

279. Consumers of healthcare value their privacy, the privacy of their dependents, and the ability to keep their PII/PHI associated with obtaining healthcare private. To customers such as Plaintiffs and Class members, healthcare that does not adhere to industry-standard data security protocols to protect PII/PHI is fundamentally less useful and less valuable than healthcare that adheres to industry-standard data security. Plaintiffs and Class members would not have entered into these contracts with 21st Century and/or its affiliated healthcare providers as a direct or third-party beneficiary without an understanding that their PII/PHI would be safeguarded and protected.

280. A meeting of the minds occurred, as Plaintiffs and members of the Class provided their PII/PHI to 21st Century and/or its affiliated healthcare providers, and paid for the provided healthcare in exchange for, amongst other things, protection of their PII/PHI.

281. 21st Century materially breached the terms of these express contracts, including, but not limited to, the terms stated in the relevant Notice of Privacy Practices. 21st Century did not "maintain the privacy" of Plaintiffs' and Class members' PII/PHI as evidenced by its notifications of the Data Breach to Plaintiffs and 2.2 million Class members.

Specifically, 21st Century did not comply with industry standards, or otherwise protect Plaintiffs' and the Class members' PII/PHI, as set forth above. Further, on information and belief, 21st Century has not yet provided Data Breach notifications to some affected Class members who may already be victims of identity fraud or theft or are at imminent risk of becoming victims of identity theft or fraud associated with PII/PHI that they provided to 21st Century. These Class members are as yet unaware of the potential source for the compromise of their PII/PHI.

282. The Data Breach was a reasonably foreseeable consequence of 21st Century's actions in breach of these contracts.

283. As a result of 21st Century's failure to fulfill the data security protections promised in these contracts, Plaintiffs and members of the Class did not receive the full benefit of the bargain, and instead received healthcare and other services that were of a diminished value to that described in the contracts. Plaintiffs and Class members, therefore, were damaged in an amount at least equal to the difference in the value of the healthcare with data security protection they paid for and the healthcare they received.

284. Had 21st Century disclosed that its security was inadequate or that it did not adhere to industry-standard security measures, neither the Plaintiffs, the Class members, nor any reasonable person would have purchased healthcare from 21st Century and/or its affiliated healthcare providers.

285. As a result of 21st Century's breach, Plaintiffs and members of the Class suffered actual damages resulting from the release, disclosure, and publication of their PII/PHI, as well as the loss of control of their PII/PHI, and remain in imminent risk of

suffering additional damages in the future.

286. Also, as a result of 21st Century's breach, Plaintiffs and the Class members have suffered actual damages resulting from their attempt to mitigate the effects of the breach of contract and subsequent Data Breach, including, but not limited to, purchasing credit monitoring and taking other steps to protect themselves from the loss of their PII/PHI.

287. Accordingly, Plaintiffs and the other members of the Class have been injured as a result of 21st Century's breach of contracts and are entitled to damages and/or restitution in an amount to be determined at trial.

COUNT V
BREACH OF IMPLIED CONTRACTS
(On Behalf of the Nationwide Class)

288. Plaintiffs incorporate all foregoing factual allegations as if fully set forth herein.

289. Plaintiffs and Class members were required to provide their PII/PHI to obtain healthcare from affiliated providers of 21st Century, and/or 21st Century. Plaintiffs and Class members entrusted their PII/PHI to 21st Century and/or its affiliated healthcare providers in order to obtain healthcare from them.

290. By providing their PII/PHI, and upon 21st Century's acceptance of such information, Plaintiffs and Class members on one hand, and 21st Century on the other hand, entered into implied contracts for the provision of adequate data security, separate and apart from any express contracts concerning health care, whereby, 21st Century was obligated to take reasonable steps to secure and safeguard that information.

291. 21st Century had an implied duty of good faith to ensure that the PII/PHI of

Plaintiffs and Class members in its possession was only used in accordance with their contractual obligations.

292. 21st Century was therefore required to act fairly, reasonably, and in good faith in carrying out its contractual obligations to protect the confidentiality of Plaintiffs' and Class members' PII/PHI and to comply with industry standards for the security of this information, and 21st Century Oncology expressly assented to these terms in its Notice of Privacy Practices as alleged above.

293. Under these implied contracts for data security, 21st Century was further obligated to provide Plaintiffs and all Class members, with prompt and sufficient notice of any and all unauthorized access and/or theft of their PII/PHI.

294. Plaintiff and Class members performed all conditions, covenants, obligations, and promises owed to 21st Century, including paying for the medical care associated with 21st Century and/or providing the PII/PHI required to 21st Century and/or its affiliate providers.

295. 21st Century breached the implied contracts by failing to take adequate measures to protect the confidentiality of Plaintiffs' and Class members' PII/PHI, resulting in the release, disclosure, and publication of their PII/PHI. 21st Century unreasonably interfered with the contract benefits owed to Plaintiffs and Class members.

296. Further, on information and belief, 21st Century has not yet provided Data Breach notifications to some affected Class members who may already be victims of identity fraud or theft or are at imminent risk of becoming victims of identity theft or fraud associated with the PII/PHI that they provided to 21st Century. These Class members are unaware of the

potential source for the compromise of their PII/PHI.

297. The Data Breach was a reasonably foreseeable consequence of 21st Century's actions in breach of these contracts.

298. As a result of 21st Century's conduct, Plaintiffs and members of the Class did not receive the full benefit of the bargain, and instead received healthcare that was of a diminished value to the healthcare with data security protection they paid for. Plaintiffs and Class members, therefore, were damaged in an amount at least equal to the difference in the value of the healthcare with data security protection they paid for and the healthcare they received.

299. Neither Plaintiffs, Class members, nor any reasonable person would have provided their PII/PHI to 21st Century and/or its affiliate providers had 21st Century disclosed that its security was inadequate or that it did not adhere to industry-standard security measures.

300. As a result of 21st Century's breach, Plaintiffs and members of the Class have suffered actual damages resulting from the release, disclosure, and publication of their PII/PHI as well as the loss of control of their PII/PHI, and remain in imminent risk of suffering additional damages in the future.

301. Also, as a result of 21st Century's breach, Plaintiffs and the Class members have suffered actual damages resulting from their attempt to mitigate the effect of the breach of implied contract and subsequent Data Breach, including, but not limited, to purchasing credit monitoring and taking other steps to protect themselves from the impermissible release, disclosure, and publication of their PII/PHI. As a result, Plaintiffs and the Class

members have suffered actual identity theft and the loss of control their PII/PHI.

302. Accordingly, Plaintiffs and Class members have been injured as a result of 21st Century's breach of implied contracts and are entitled to damages and/or restitution in an amount to be proven at trial.

COUNT VI
BREACH OF IMPLIED DUTY OF GOOD FAITH AND FAIR DEALING
(On Behalf of the Nationwide Class)

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

304. Plaintiffs and Class members entered into and/or were the beneficiaries of contracts with Defendants and their affiliates, as alleged above.

305. 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 Defendants and their affiliates would act fairly, reasonably, and in good faith in carrying out their contractual obligations to protect the confidentiality of Plaintiffs' and Class members' PII/PHI and to comply with industry standards for the security of this information.

306. Special relationships exist between Defendants and their affiliates and Plaintiffs and Class members. Defendants and their affiliates entered into special relationships with Plaintiffs and Class members who entrusted their confidential PII/PHI to Defendants and their affiliates and paid for medical services with Defendants.

307. Defendants and their affiliates promised and were obligated to protect the confidentiality of Plaintiffs' and Class members' PII/PHI from release, disclosure, and publication. Defendants 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/PHI, which resulted in the release, disclosure, and publication of this PII/PHI. Defendants unreasonably interfered with the contract benefits owed to Plaintiffs and Class members by failing to implement reasonable and adequate security measures consistent with industry standards to protect and limit impermissible release, disclosure, and publication of Plaintiffs' and Class members' PII/PHI.

308. Plaintiffs and Class members performed all conditions, covenants, obligations, and promises owed to Defendants, including paying Defendants and their affiliates for medical services and providing them the confidential PII/PHI required by the contracts.

309. As a result of Defendants' breach of the implied covenant of good faith and fair dealing, Plaintiffs and Class members did not receive the full benefit of their bargain—medical services with reasonable data privacy—and instead received medical services that were less valuable than what they paid for and less valuable than what they reasonably expected under the contracts. Plaintiffs and Class members have suffered actual damages in an amount equal to the difference in the value between medical care with reasonable data privacy that Plaintiffs and Class members paid for, and the medical care they received without reasonable data privacy.

310. As a result of Defendants' breach of the implied covenant of good faith and fair dealing, Plaintiffs and Class members have suffered actual damages resulting from the

impermissible release, disclosure, and publication of their PII/PHI and remain at imminent risk of suffering additional damages in the future.

311. As a result of Defendants' breach of the implied 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, including, but not limited to, purchasing credit monitoring services or taking other steps to protect themselves from the impermissible release, disclosure, and publication of their PII/PHI.

312. As a direct and proximate cause of Defendants' conduct, Plaintiffs and Class members suffered injury in fact and are therefore entitled to relief, including restitution, declaratory relief, and a permanent injunction enjoining Defendants from their conduct.

COUNT VII
BREACH OF FIDUCIARY DUTY
(On Behalf of the Nationwide Class)

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

314. Defendants owed a fiduciary duty to Plaintiffs and the Class as guardians of their PII/PHI to (a) protect the PII/PHI belonging to Plaintiffs and members of the Class; and (b) timely notify them of the Data Breach.

315. Defendants breached their fiduciary duty to Plaintiffs and the Class by (a) failing to adequately secure their PII/PHI from impermissible release, disclosure, and publication; (b) failing to take adequate actions to prevent release, disclosure, and publication of Plaintiffs' and Class members' PII/PHI in a manner that would be highly offensive to a reasonable person; (c) failing to take adequate actions to prevent release, disclosure, and

publication of Plaintiffs' and Class members' PII/PHI to unauthorized parties without the informed and clear consent of Plaintiffs and the Class; (d) failing to take adequate actions to prevent improper release, disclosure, and publication of Plaintiffs' and Class members' PII/PHI that would be highly offensive to a reasonable person; and (e) notifying Plaintiffs and the Class of the Data Breach five months after it had occurred and four months after Defendants had knowledge of the Data Breach..

316. As a direct and proximate cause of Defendants' conduct, Plaintiffs and Class members suffered an injury in fact and are therefore entitled to relief, including restitution, declaratory relief, and a permanent injunction enjoining Defendants from their conduct.

COUNT VIII
UNJUST ENRICHMENT
(Alternative to Breach of Contract Claim)
(On Behalf of the Nationwide Class)

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

318. Plaintiffs and Class members conferred a monetary benefit on Defendants in the form of monetary payments—directly or indirectly—for medical services received.

319. Defendants collected, maintained, and stored the PII/PHI of Plaintiffs and Class members and, as such, Defendants had knowledge of the monetary benefits conferred by Plaintiffs and Class members.

320. The money that Plaintiffs and Class members paid to Defendants should have been used to pay, at least in part, for the administrative costs and implementation of data security adequate to safeguard and protect the confidentiality of Plaintiffs' and Class members' PII/PHI. Defendants failed to implement—or adequately implement—adequate

data security practices, procedures, and programs to secure sensitive PII/PHI, as evidenced by the Data Breach.

321. As a result of Defendants' failure to implement data security practices, procedures, and programs to secure sensitive PII/PHI, Plaintiffs and Class members suffered actual damages in an amount equal to the difference in the value between medical care with reasonable data privacy that Plaintiffs and Class members paid for, and the medical care they received without reasonable data privacy.

322. Under principles of equity and good conscience, Defendants should not be permitted to retain the money belonging to Plaintiffs and Class members because Defendants failed to implement the data security measures adequate to safeguard and protect the confidentiality of Plaintiffs' and Class members' PII/PHI and that Plaintiffs and Class members paid for.

323. Defendants should be compelled to disgorge into a common fund for the benefit of Plaintiffs and the Class all unlawful or inequitable proceeds received by Defendants. A constructive trust should be imposed upon all unlawful and inequitable sums received by Defendants traceable to Plaintiffs and the Class.

COUNT IX
INVASION OF PRIVACY
(On Behalf of the Nationwide Class)

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

325. Plaintiffs and Class members reasonably expected that their PII/PHI would be protected and secured from release, disclosure, and publication, and that their PII/PHI would

not be released, disclosed, or published for any improper purpose.

326. Defendants unlawfully invaded the privacy rights of Plaintiffs and the Class by (a) failing to adequately secure their PII/PHI from release, disclosure, and publication; (b) failing to take adequate actions to prevent the release, disclosure, and publication of Plaintiffs' and Class members' PII/PHI; and (c) releasing, disclosing, and publishing their PII/PHI.

327. Defendants' actions and omissions resulted in the release, disclosure, and publication of Plaintiffs' and Class members' PII/PHI.

328. The release, disclosure, and publication of Plaintiffs' and Class members' PII/PHI occurred without the informed and clear consent of Plaintiffs and Class members.

329. The release, disclosure, and publication of Plaintiffs' and Class members' PII/PHI would be highly offensive and objectionable to a reasonable person.

330. The private facts, including PII/PHI, that were released, disclosed, and published are not a matter of public concern.

331. In failing to adequately secure Plaintiffs' and Class members' PII/PHI, Defendants acted in reckless disregard of their privacy rights. Defendants knew or should have known that their substandard data security measures would be highly offensive to a reasonable person in the same position as Plaintiffs and Class members.

332. Defendants violated Plaintiffs' and Class members' right to privacy under the common law and state constitutions, including, but not limited to, Article I, Section I of the California Constitution.

333. As a direct and proximate result of Defendants' unlawful invasions of privacy,

Plaintiffs' and Class members' PII/PHI has been viewed or is at imminent risk of being viewed, and their reasonable expectations of privacy have been intruded upon and frustrated. Plaintiffs and the Class have suffered injury as a result of Defendants' unlawful invasions of privacy and are entitled to appropriate relief.

COUNT X
DECLARATORY JUDGMENT
(On Behalf of the Nationwide Class)

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

335. Plaintiffs and the Class have stated claims against Defendants based on negligence, gross negligence, negligent misrepresentation, breach of express contract, breach of implied contracts, breach implied duty of good faith and fair dealing, breach of fiduciary duty, unjust enrichment, and invasion of privacy.

336. Defendants failed to fulfill their obligations to provide adequate and reasonable data security measures for the PII/PHI of Plaintiffs and the Class, as evidenced by the Data Breach.

337. As a result of the Data Breach, Defendants' system is more vulnerable to access by unauthorized parties and requires more stringent measures to be taken to safeguard the PII/PHI of Plaintiffs and the Class going forward.

338. An actual controversy has arisen in the wake of the Data Breach regarding Defendants' current obligations to provide data security measures adequate to protect the PII/PHI of Plaintiffs and the Class. Defendants maintain that their security measures were—and still are—reasonably adequate and denies that they previously had or have any obligation

to implement better safeguards to protect the PII/PHI of Plaintiffs and the Class.

339. Plaintiffs seek a declaration that Defendants must implement specific additional, prudent, industry-standard data security practices to provide reasonable protection and security to the PII/PHI of Plaintiffs and the Class. Specifically, Plaintiffs and the Class seek a declaration that Defendants' existing security measures do not comply with their obligations, and that Defendants must implement and maintain reasonable data security measures on behalf of Plaintiffs and the Class to comply with their data security obligations.

VIII. PRAYER FOR RELIEF

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

(a) Certify this case as a class action, appoint Plaintiffs as class representatives, and appoint Interim Co-Lead Counsel, Plaintiffs' Liaison Counsel, Plaintiffs' Local Counsel, and Plaintiffs' Steering Committee as Class Counsel for Plaintiffs to represent the Class;

(b) Find that 21st Century breached its duty to safeguard and protect the PII/PHI of Plaintiffs and Class members that was compromised in the Data Breach;

(c) Award Plaintiffs and Class members appropriate relief, including actual 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 DEMANDED

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

Dated: July 30, 2018

Respectfully submitted,

By: */s/ Cari Campen Laufenberg*
Cari Campen Laufenberg
KELLER ROHRBACK L.L.P.
1201 Third Avenue, Suite 3200
Seattle, WA 98101
Telephone: (206) 623-1900
Facsimile: (206) 623-3384
claufenberg@kellerrohrback.com

By: */s/ Daniel S. Robinson*
Daniel S. Robinson
ROBINSON CALCAGNIE, INC.
19 Corporate Plaza Drive
Newport Beach, California 92660
Telephone: (949) 720-1288
Facsimile: (949) 720-1292
drobinson@robinsonfirm.com

Interim Co-Lead Counsel for Plaintiffs

Jodi Westbrook Flowers
MOTLEY RICE LLC
28 Bridgeside Blvd.
Mt. Pleasant, SC 29464
Telephone: (843) 216-9000
Facsimile: (843) 216-9450
jflowers@motleyrice.com

Robert C. Gilbert
Florida Bar No. 561861
KOPELOWITZ OSTROW 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

Interim Co-Liaison Counsel for Plaintiffs

Kent G. Whittemore
Florida Bar No. 166049
THE WHITTEMORE LAW GROUP, P.A.
100 Second Avenue South, Ste. 304-S
St. Petersburg, FL 33701
Telephone: (727) 821-8752
kwhittemore@wherejusticematters.com

Interim Local Counsel for Plaintiffs

Matthew B. George
KAPLAN FOX & KILSHEIMER LLP
350 Sansome Street, Suite 400
San Francisco, CA 94104
Telephone: (415) 772-4700
Facsimile: (415) 772-4707
mgeorge@kaplanfox.com

Kenneth G. Gilman
Florida Bar No. 340758
GILMAN LAW, LLP
Beachway Professional Center Tower
8951 Bonita Beach Road, S.E. Ste. #525
Bonita Springs, FL 34135
Telephone: (239) 494-6128
kgilman@gilmanlawllp.com

Thomas V. Girardi
GIRARDI | KEESE
1126 Wilshire Boulevard
Los Angeles, CA 90017
Telephone: (213) 977-0211
Facsimile: (213) 481-1554
tgirardi@girardikeese.com

Eric A. Grover
KELLER GROVER LLP
1965 Market Street
San Francisco, CA 94103
Telephone: (415) 543-1305
Facsimile: (415) 543-7861
eagrover@kellergrover.com

Julie Braman Kane
Florida Bar No. 980277
COLSON HICKS EIDSON, P.A.
255 Alhambra Circle, Penthouse
Coral Gables, Florida 33134
Telephone: (305) 476-7400
Facsimile: (305) 476-7444
julie@colson.com

Steven S. Maher
Florida Bar No. 887846
THE MAHER LAW FIRM, PA
631 W Morse Blvd., Suite 200
Winter Park, FL 32789
Telephone: (407) 839-0866
Facsimile: (407) 425-7958
smaher@maherlawfirm.com

Charles PT Phoenix
Florida Bar No. 0535591
RHODES TUCKER
2407 Periwinkle Way, Suite 6
Sanibel, FL 33957
Telephone: (239) 472-1144
Facsimile: (239) 461-0083
cptp@RhodesTucker.com

Daniel Girard
GIRARD GIBBS LLP
601 California St., 14th Floor
San Francisco, CA 94108
Telephone: (415) 981-4800
Facsimile: (415) 981-4846
lgv@girardgibbs.com

Plaintiffs' Steering Committee