UNITED STATES DISTRICT COURT
FOR THE MIDDLE DISTRICT OF PENNSYLVANIA
READING DIVISION

LUGENIA BOOKER, Individually and on behalf of all others similarly situated, Plaintiff, v. PERSONAL TOUCH HOLDING CORP., and CROSSROADS TECHNOLOGIES, INC. Defendants.	**CASE NO.** **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

1. Plaintiff LUGENIA BOOKER, individually and on behalf of all others similarly situated, brings this action against Defendants PERSONAL TOUCH HOLDING CORP. ("Personal Touch" and collectively "Defendants") and CROSSROADS TECHNOLOGIES, INC. ("Crossroads" and collectively "Defendants") to obtain damages, restitution, and injunctive relief for the Class, as defined below, from Defendants. Plaintiff makes the following allegations upon information and belief, except as to her own actions, the investigation of her counsel, and the facts that are a matter of public record:

JURISDICTION AND VENUE

2. This Court has jurisdiction over this action under the Class Action Fairness Act ("CAFA"), 28 U.S.C. § 1332(d). There are at least 100 members in the proposed class, the aggregated claims of the individual Class Members exceed the sum or value of $5,000,000.00

exclusive of interest and costs, and members of the Proposed Class (such as named Plaintiff Booker) are citizens of states different from Defendants.

3. Defendant Personal Touch has sufficient minimum contacts in Pennsylvania, as it does business in the Commonwealth of Pennsylvania (through, among other things, its affiliate entity Personal Touch Home Care of PA, Inc.), and the business being done in Pennsylvania directly relates to the subject of this lawsuit (in that Personal Touch Home Care of PA, Inc was one of the Personal Touch entities whose data was breached), thus rendering the exercise of personal jurisdiction by this Court proper and necessary.

4. Defendant Crossroads has sufficient minimum contacts in Pennsylvania, as it is a domestic corporation organized under the laws of the Commonwealth of Pennsylvania and has its principal place of business in Pennsylvania, thus rendering the exercise of personal jurisdiction by this Court proper and necessary.

5. Venue is proper in this District under 28 U.S.C. § 1391 because a substantial part of the events and omissions giving rise to these claims occurred in this District.

NATURE OF THIS ACTION

6. This class action arises out of the recent ransomware attack that was perpetrated against Defendant Crossroads, which held in its "cloud" personal and confidential information (including Protected Health Information) of Defendant Personal Touch's patients. The cyberattack subsequently disrupted operations at Defendant Personal Touch by, among other things, blocking access to Personal Touch's data that was being held by Defendant Crossroads, including the highly sensitive patient medical records of 156,409 patients (the "Ransomware Attack"). As a result of the Ransomware Attack, Plaintiff and Class Members suffered ascertainable losses in the form of disruption of medical services, out-of-pocket expenses

and the value of their time reasonably incurred to remedy or mitigate the effects of the attack. In addition, Plaintiff's and Class Members' sensitive personal information—which was entrusted to Personal Touch, its officials and agents (including its agent Defendant Crossroads)—was compromised and unlawfully accessed due to the Ransomware Attack. Information compromised in the Ransomware Attack includes patient names, addresses, telephone numbers, dates of birth, medical record information, health insurance card numbers, plan benefit numbers, Social Security numbers, treatment details, and other protected health information as defined by the HIPAA, and additional personally identifiable information ("PII") and protected health information ("PHI") that Defendant Personal Touch collected and that Defendant Crossroads maintained (collectively the "Private Information").

7. Plaintiff brings this class action lawsuit on behalf of those similarly situated to address Defendants' inadequate safeguarding of Class Members' Private Information that they collected and maintained, and for failing to provide timely and adequate notice to Plaintiff and other Class Members that their information had been subject to the unauthorized access of an unknown third party and precisely what specific type of information was accessed.

8. Defendants maintained the Private Information in a reckless manner. In particular, the Private Information was maintained on Defendant Crossroad's computer cloud storage network in a condition vulnerable to cyberattacks of the type that cause actual disruption to Plaintiff's and Class Members' medical care and treatment. As a result of the Ransomware Attack, Plaintiff's and Class Members' Private Information was seized and held hostage by computer hackers for "ransom," and ultimately disclosed to other unknown thieves. Upon information and belief, the mechanism of the ransomware and potential for improper disclosure of Plaintiff's and Class Members' Private Information was a known risk to Defendants, and thus Defendants were on

notice that failing to take steps necessary to secure the Private Information from those risks left that property in a dangerous condition.

9. In addition, Defendant Crossroads (acting in the course and scope of its agency relationship with Defendant Personal Touch) and its employees failed to properly monitor the computer network and systems that housed the Private Information. Had Crossroads properly monitored its property, it would have discovered the intrusion sooner.

10. Because of the Ransomware Attack, Plaintiff and Class Members had their medical care and treatment as well as their daily lives disrupted. As a consequence of the ransomware locking down the medical records of Plaintiff and Class Members, Plaintiff and Class Members had to, among other things, forego medical care and treatment or had to seek alternative care and treatment.

11. What's more, aside from having their lives disrupted, Plaintiff's and Class Members' identities are now at risk because of Defendants' negligent conduct since the Private Information that Defendant Personal Touch collected and Defendant Crossroads maintained is now in the hands of data thieves.

12. Armed with the Private Information accessed in the Ransomware Attack, data thieves can commit a variety of crimes including, e.g., opening new financial accounts in class members' names, taking out loans in class members' names, using class members' names to obtain medical services, using class members' health information to target other phishing and hacking intrusions based on their individual health needs, using class members' information to obtain government benefits, filing fraudulent tax returns using class members' information, obtaining driver's licenses in class members' names but with another person's photograph, and giving false information to police during an arrest.

13. As a further result of the Ransomware Attack, Plaintiff and Class Members have been exposed to a heightened and imminent risk of fraud and identity theft. Plaintiff and Class Members must now and in the future closely monitor their financial accounts to guard against identity theft.

14. Plaintiff and Class Members may also incur out of pocket costs for, e.g., purchasing credit monitoring services, credit freezes, credit reports, or other protective measures to deter and detect identity theft.

15. By her Complaint, Plaintiff seeks to remedy these harms on behalf of herself and all similarly situated individuals whose Private Information was accessed or ransomed during the Ransomware Attack.

16. Plaintiff seeks remedies including, but not limited to, compensatory damages, reimbursement of out-of-pocket costs, and injunctive relief including improvements to Defendants' data security systems, future annual audits, and adequate credit monitoring services funded by Defendants.

17. Accordingly, Plaintiff brings this action against Defendants seeking redress for their unlawful conduct asserting claims for negligence, an intrusion upon seclusion, breach of an express and implied contract, unjust enrichment, and breach of fiduciary duty.

PARTIES

18. Plaintiff LUGENIA BOOKER is and at all times mentioned herein was an individual citizen of the State of New York residing in the City of Far Rockaway.

19. Defendant Personal Touch is a Delaware corporation with its principal place of business at 222-15 Northern Blvd., Bayside, New York 11361.

20. Defendant Personal Touch is the holding company for a number of home health care entities, all of which operate under the "Personal Touch" name, and which include the following entities:

a. Personal Touch Home Care of VA, Inc.

b. Personal Touch Home Care of W. VA, Inc.

c. Personal Touch Hospice of VA, Inc.

d. Personal Touch Home Care of Mass., Inc.

e. PT Home Services of San Antonio, Inc.

f. Personal Touch Home-Aides, Inc.

g. Personal Touch Home Services of Dallas, Inc.

h. Personal Touch Home Care of S.E. Mass., Inc.

i. Personal Touch Home Aides Inc.

j. Personal Touch Home Care of PA, Inc.

k. Personal Touch Home Care of Ohio, Inc.

l. Personal Touch Home Care of Greater Portsmouth, Inc.

m. Personal Touch Home Aides of Baltimore, Inc.

n. Personal Touch Home Care of Baltimore, Inc.

o. Personal Touch Home Care of KY, Inc.

p. Personal Touch Home Care of Indiana, Inc., and

q. Personal Touch Home Aides of New York, Inc.

21. Defendant Crossroads is a Pennsylvania domestic corporation with its principal place of business at 3 Park Plaza, Suite 305, Wyomissing, PA 19610 (Berks County).

DEFENDANTS' BUSINESSES

22. Personal Touch is a nationwide network of home health care providers, operating through a network of subsidiaries and affiliate business entities that are each licensed in the state in which services are provided.

23. Defendant Personal Touch provides comprehensive home health to patients from across the country.

24. Services offered by Defendant Personal Touch include, but are not limited to, the following: Home Health Aides, Personal Care Aides, Nursing Services, Physical Therapy, Occupational Therapy, Hospice, Homemaker/Home keeper, Speech Language Pathology, Occupational Therapy, Psychiatric Nursing, Pediatric Care, Early Intervention Services, Wound Care, and Post Surgery Care.

25. In the ordinary course of receiving home health care services from Defendant Personal Touch, patients provide Defendant Personal Touch with sensitive, personal and private information such as:

- Name, address, phone number and email address;
- Dates of birth;
- Social Security numbers;
- Information relating to individual medical history;
- Medical record information;
- Insurance information and coverage, and;
- Treatment details

26. All of Defendant Personal Touch's employees, staff, entities, sites, and locations may share patient information with each other for various purposes, as disclosed in the HIPAA compliant privacy notice that Defendant Personal Touch is required to maintain.

27. The Privacy Policy is posted on Defendant Personal Touch's website, and is provided to every patient upon request.[1]

28. Because of the highly sensitive and personal nature of the information Defendant Personal Touch acquires and stores with respect to its home health care patients, Defendant Personal Touch promises to: (1) maintain the privacy and security of patients' protected health information; (2) promptly notify patients if a breach occurs that may have compromised the privacy or security of patient information; (3) follow the duties and privacy practices described in the privacy notice and give patients a copy of it, and; (4) not use or share patient information other than as described in the privacy notice unless patients tell Defendant Personal Touch it can do so in writing.

29. Upon information and belief, Defendant Personal Touch contracted with Defendant Crossroads to provide cloud-based computer storage for the highly personal and highly sensitive information it collects about its patients.

30. Under the terms of the contract, Defendant Crossroads became Defendant Personal Touch's agent for the purposes of storing, maintaining, and guarding this highly personal, highly sensitive, and highly confidential patient information.

31. Under the terms of the contract, Defendant Crossroads agreed to and undertook legal duties to maintain the protected health information entrusted to it by Defendant Personal

[1] https://www.pthomecare.com/privacy-practices

Touch safely, confidentially, and in compliance with all applicable laws, including the Health Insurance Portability and Accountability Act ("HIPAA").

32. Defendant Crossroads held the patient information collected by Defendant Personal Touch at Crossroads' Wyomissing, Pennsylvania data center in an electronic medical records system that Crossroads hosts.[2]

33. The patient information held by Defendant Crossroads in its hosted electronic medical records system included the protected health information of Plaintiff and Class Members.

THE RANSOMWARE ATTACK

34. A ransomware attack is a type of malicious software that blocks access to a computer system or data, usually by encrypting it, until the victim pays a fee to the attacker.[3]

35. At some point prior to December 1, 2019, ransomware was deployed on Defendant Crossroads' hosted electronic medical records system which resulted in widespread file encryption of files containing Protected Health Information that had been collected by Defendant Personal Touch.[4]

36. Crossroads advised Personal Touch on December 1, 2019 that the ransomware attack impacted its Pennsylvania data center where Personal Touch's electronic medical records were held.

37. The Ransomware Attack stopped patient records from being viewed for a number of days, causing disruption to medical care and treatment.

[2] https://www.compliancejunction.com/156400-people-have-phi-breached-in-personal-touch-home-care-patients-ransomware-attack/
[3] https://www.proofpoint.com/us/threat-reference/ransomware.
[4] https://ago.vermont.gov/blog/2020/01/28/personal-touch-holding-corp-personal-touch-home-care-of-greater-portsmouth-notice-of-data-breach-to-consumers/

38. While Crossroads' electronic health records system was offline, staff at Personal Touch were forced to use emergency protocols and employed pen and paper to record patient data.

39. The compromised medical records included patient names, addresses, telephone numbers, dates of birth, medical record information, health insurance card numbers, plan benefit numbers, Social Security numbers, and treatment details.

40. The Personal Touch offices affected included:

a. Personal Touch Home Care of VA, Inc.

b. Personal Touch Home Care of W. VA, Inc.

c. Personal Touch Hospice of VA, Inc.

d. Personal Touch Home Care of Mass., Inc.

e. PT Home Services of San Antonio, Inc.

f. Personal Touch Home-Aides, Inc.

g. Personal Touch Home Services of Dallas, Inc.

h. Personal Touch Home Care of S.E. Mass., Inc.

i. Personal Touch Home Aides Inc.

j. Personal Touch Home Care of PA, Inc.

k. Personal Touch Home Care of Ohio, Inc.

l. Personal Touch Home Care of Greater Portsmouth, Inc.

m. Personal Touch Home Aides of Baltimore, Inc.

n. Personal Touch Home Care of Baltimore, Inc.

o. Personal Touch Home Care of KY, Inc.

p. Personal Touch Home Care of Indiana, Inc., and

q. Personal Touch Home Aides of New York, Inc.

41. The incident was made known to the Department of Health and Human Services' Office for Civil Rights.

42. Overall, the PHI of 156,409 patients and caregivers across 6 states was impacted.

43. Notification letters were sent to affected patients beginning on January 28, 2020.[5]

44. Defendants had obligations created by HIPAA, contract, industry standards, common law, and representations made to Class Members, to keep Class Members' Private Information confidential and to protect it from unauthorized access and disclosure.

45. Plaintiff and Class Members provided their Private Information to Defendants with the reasonable expectation and mutual understanding that Defendants would comply with their obligations to keep such information confidential and secure from unauthorized access.

46. Defendants' data security obligations were particularly important given the substantial increase in ransomware attacks and/or data breaches in the healthcare industry preceding the date of the breach.

47. Indeed, ransomware attacks, such as the one experienced by Defendant Crossroads, have become so notorious that the Federal Bureau of Investigation ("FBI") and U.S. Secret Service have issued a warning to potential targets so they are aware of, and prepared for, a potential attack. As one report explained, "[e]ntities like smaller municipalities and hospitals are attractive to ransomware criminals…because they often have lesser IT defenses and a high incentive to regain access to their data quickly."

[5] https://ago.vermont.gov/blog/2020/01/28/personal-touch-holding-corp-personal-touch-home-care-of-greater-portsmouth-notice-of-data-breach-to-consumers/

48. Therefore, the increase in such attacks, and attendant risk of future attacks, was widely known to the public and to anyone in Defendants' industries, including Defendants Personal Touch and Crossroads.

49. Defendants breached their obligations to Plaintiff and Class Members and/or were otherwise negligent and reckless because they failed to properly maintain and safeguard the Crossroads' computer systems and the Personal Touch data. Defendants' unlawful conduct includes, but is not limited to, the following acts and/or omissions:

a. Failing to maintain an adequate data security system to reduce the risk of data breaches and cyber-attacks;

b. Failing to adequately protect patients' Private Information;

c. Failing to properly monitor their own data security systems for existing intrusions;

d. Failing to ensure that vendors with access to Personal Touch's protected health data employed reasonable security procedures;

e. Failing to ensure the confidentiality and integrity of electronic PHI it created, received, maintained, and/or transmitted, in violation of 45 C.F.R. § 164.306(a)(1);

f. Failing to implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights in violation of 45 C.F.R. § 164.312(a)(1);

g. Failing to implement policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 C.F.R. § 164.308(a)(1)(i);

h. Failing to implement procedures to review records of information system activity regularly, such as audit logs, access reports, and security incident tracking reports in violation of 45 C.F.R. § 164.308(a)(1)(ii)(D);

i. Failing to protect against reasonably anticipated threats or hazards to the security or integrity of electronic PHI in violation of 45 C.F.R. § 164.306(a)(2);

j. Failing to protect against reasonably anticipated uses or disclosures of electronic PHI that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 C.F.R. § 164.306(a)(3);

k. Failing to ensure compliance with HIPAA security standard rules by Defendants' workforces in violation of 45 C.F.R. § 164.306(a)(4);

l. Failing to train all members of Defendants' workforces effectively on the policies and procedures regarding PHI as necessary and appropriate for the members of their workforces to carry out their functions and to maintain security of PHI, in violation of 45 C.F.R. § 164.530(b); and/or

m. Failing to render the electronic PHI it maintained unusable, unreadable, or indecipherable to unauthorized individuals, as it had not encrypted the electronic PHI as specified in the HIPAA Security Rule by "the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key" (45 CFR 164.304 definition of encryption).

50. As the result of computer systems in dire need of security upgrading, inadequate procedures for handling emails containing ransomware or other malignant computer code, and

inadequately trained employees who opened files containing the ransomware virus, Defendants negligently and unlawfully failed to safeguard Plaintiff's and Class Members' Private Information.

51. Accordingly, as outlined below, Plaintiff's and Class Members' health care and daily lives were severely disrupted. What's more, they now face an increased risk of fraud and identity theft.

RANSOMWARE ATTACKS AND DATA BREACHES CAUSE DISRUPTION AND PUT CONSUMERS AT AN INCREASED RISK OF FRAUD AND IDENTIFY THEFT

52. Ransomware attacks such as this one are especially problematic because of the disruption they cause to the medical treatment and overall daily lives of patients affected by the attack.

53. For instance, loss of access to patient histories, charts, images and other information forces providers to limit or cancel patient treatment because of the disruption of service.

54. This leads to a deterioration in the quality of overall care patients receive at facilities affected by ransomware attacks and related data breaches.

55. Researchers have found that at medical facilities that experienced a data security incident, the death rate among patients increased in the months and years after the attack.[6]

56. Researchers have further found that at medical facilities that experienced a data security incident, the incident was associated with deterioration in patient outcomes, generally.[7]

[6] *See* https://www.pbs.org/newshour/science/ransomware-and-other-data-breaches-linked-to-uptick-in-fatal-heart-attacks

[7] *See* https://onlinelibrary.wiley.com/doi/full/10.1111/1475-6773.13203.

57. Similarly, ransomware attacks and related data security incidents inconvenience patients. Inconveniences patients encounter as a result of such incidents include, but are not limited, to the following:

a. rescheduling medical treatment;

b. finding alternative medical care and treatment;

c. delaying or foregoing medical care and treatment;

d. undergoing medical care and treatment without medical providers having access to a complete medical history and records; and

e. losing patient medical history.

58. Ransomware attacks also constitute data breaches in the traditional sense. For example, in a recent ransomware attack on the Florida city of Pensacola, and while the City was still recovering from the ransomware attack, hackers released 2GB of data files from the total 32GB of data that they claimed was stolen prior to encrypting the City's network with the maze ransomware. In the statement given to a news outlet, the hackers said, "***This is the fault of mass media who writes that we don't exfiltrate data***…."[8]

59. Also, in a ransomware advisory, the Department of Health and Human Services informed entities covered by HIPAA that "when electronic protected health information (ePHI) is encrypted as the result of a ransomware attack, a breach has occurred because the ePHI encrypted by the ransomware was acquired (i.e., unauthorized individuals have taken possession or control of the information)."[9]

[8] https://www.cisomag.com/pensacola-ransomware-hackers-release-2gb-data-as-a-proof/
[9] *See* https://www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf.

60. Ransomware attacks are also considered a breach under the HIPAA Rules because there is an access of PHI not permitted under the HIPAA Privacy Rule:

> A breach under the HIPAA Rules is defined as, "...the acquisition, access, use, or disclosure of PHI in a manner not permitted under the [HIPAA Privacy Rule] which compromises the security or privacy of the PHI." See 45 C.F.R. 164.40[10]

61. Other security experts agree that when a ransomware attack occurs, a data breach does as well, because such an attack represents a loss of control of the data within a network.

62. Ransomware attacks are also Security Incidents under HIPAA because they impair both the integrity (data is not interpretable) and availability (data is not accessible) of patient health information:

> The presence of ransomware (or any malware) on a covered entity's or business associate's computer systems is a security incident under the HIPAA Security Rule. A security incident is defined as the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system. See the definition of security incident at 45 C.F.R. 164.304. Once the ransomware is detected, the covered entity or business associate must initiate its security incident and response and reporting procedures. See 45 C.F.R.164.308(a)(6).[11]

63. Data breaches represent yet another problem for patients who have already experienced inconvenience and disruption associated with a ransomware attack.

64. The United States Government Accountability Office released a report in 2007 regarding data breaches ("GOA Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[12]

---

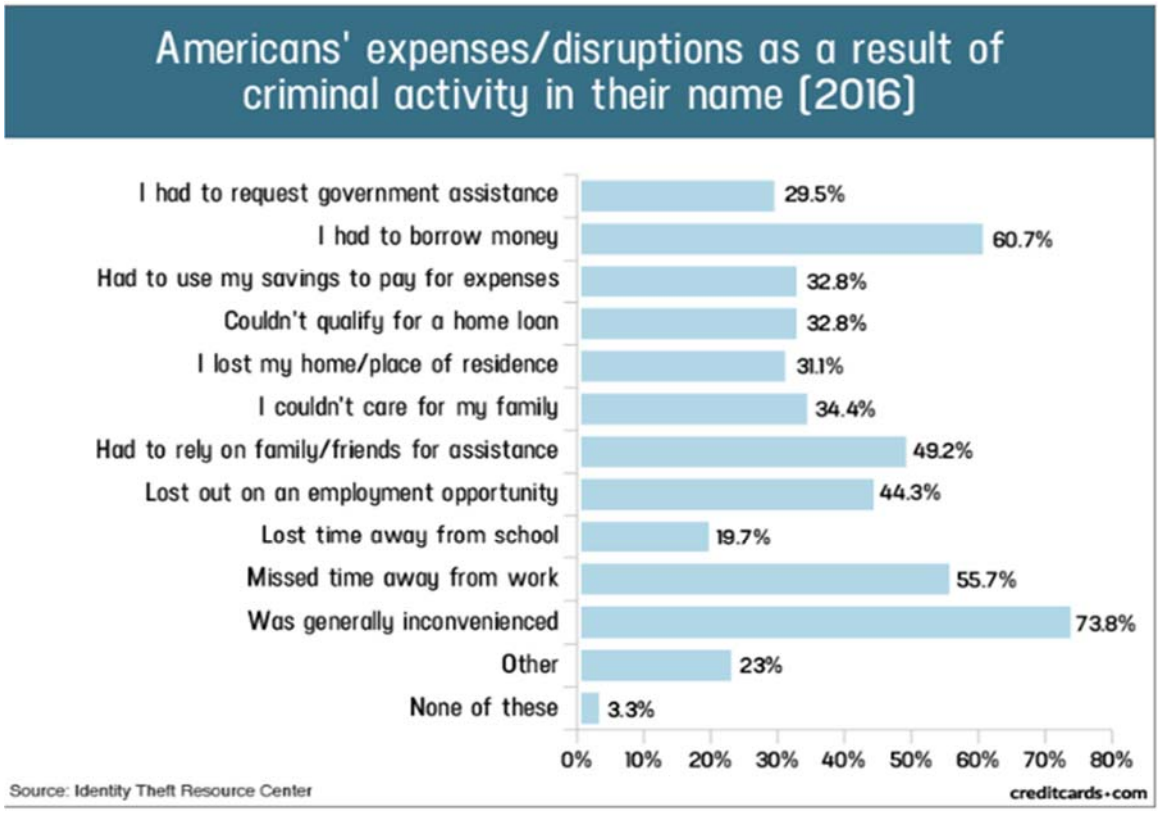
[10] See https://onlinelibrary.wiley.com/doi/full/10.1111/1475-6773.13203
[11] See https://www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf
[12] See "Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown," p. 2, U.S. Government Accountability Office, June 2007, https://www.gao.gov/new.items/d07737.pdf (last visited Apr. 12, 2019) ("GAO Report").

65. The FTC recommends that identity theft victims take several steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for 7 years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[13]

66. Identity thieves use stolen personal information such as Social Security numbers for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.

67. Identity thieves can also use Social Security numbers to obtain a driver's license or official identification card in the victim's name but with the thief's picture; use the victim's name and Social Security number to obtain government benefits; or file a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's Social Security number, rent a house or receive medical services in the victim's name, and may even give the victim's personal information to police during an arrest resulting in an arrest warrant being issued in the victim's name. A study by Identity Theft Resource Center shows the multitude of harms caused by fraudulent use of personal and financial information:[14]

[13] See https://www.identitytheft.gov/Steps (last visited April 12, 2019).
[14] "Credit Card and ID Theft Statistics" by Jason Steele, 10/24/2017, at: https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276.php (last visited June 20, 2019).



68. What's more, theft of Private Information is also gravely serious. PII/PHI is a valuable property right.[15] Its value is axiomatic, considering the value of Big Data in corporate America and the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that Private Information has considerable market value.

69. Theft of PHI, in particular, is gravely serious: "A thief may use your name or health insurance numbers to see a doctor, get prescription drugs, file claims with your insurance provider, or get other care. If the thief's health information is mixed with yours, your treatment, insurance

[15] See, e.g., John T. Soma, et al, Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

and payment records, and credit report may be affected."[16] Drug manufacturers, medical device manufacturers, pharmacies, hospitals and other healthcare service providers often purchase PII/PHI on the black market for the purpose of target marketing their products and services to the physical maladies of the data breach victims themselves. Insurance companies purchase and use wrongfully disclosed PHI to adjust their insureds' medical insurance premiums.

70. It must also be noted there may be a substantial time lag – measured in years -- between when harm occurs versus when it is discovered, and also between when Private Information and/or financial information is stolen and when it is used. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

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

See GAO Report, at p. 29.

71. Private Information and financial information are such valuable commodities to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black-market" for years.

72. There is a strong probability that entire batches of stolen information have been dumped on the black market and are yet to be dumped on the black market, meaning Plaintiff and Class Members are at an increased risk of fraud and identity theft for many years into the future. Thus, Plaintiff and Class Members must vigilantly monitor their financial and medical accounts for many years to come.

[16] See Federal Trade Commission, Medical Identity Theft, http://www.consumer.ftc.gov/articles/0171-medical-identity-theft (last visited March 27, 2020).

73. Medical information is especially valuable to identity thieves. According to account monitoring company LogDog, coveted Social Security numbers were selling on the dark web for just $1 in 2016 – the same as a Facebook account. That pales in comparison with the asking price for medical data, which was selling for $50 and up.[17]

74. Because of its value, the medical industry has experienced disproportionally higher numbers of data theft events than other industries. Defendants therefore knew or should have known this and strengthened their data systems accordingly. Defendants were put on notice of the substantial and foreseeable risk of harm from a data breach, yet they failed to properly prepare for that risk.

PLAINTIFF'S AND CLASS MEMBERS' DAMAGES

75. To date, Defendants have done absolutely nothing to provide Plaintiff and the Class Members with relief for the damages they have suffered as a result of the Ransomware Attack, including, but not limited to, the costs and conveniences they incurred because of the disruption of services from Defendant Personal Touch. Nor have Defendants offered any protection against the likely and probable effects that will result from Plaintiff's and Class Members' Private Information being stolen in connection with the attack. No credit monitoring or identity theft protection was offered in the notice of breach letter. Upon information and belief, no credit monitoring or identity theft protection has been ever offered.

76. Rather than admitting the known risks to Plaintiff and Class Members, risks that can persist for multiple years after a ransomware attack, Defendants are providing consumers like

[17] https://nakedsecurity.sophos.com/2019/10/03/ransomware-attacks-paralyze-and-sometimes-crush-hospitals/#content

Plaintiff with false assurances that their Private Information has not been misused or removed from Defendant Crossroads' computer system.

77. Instead, Defendant Personal Health actively encouraged Plaintiff and the Class Members to spend their personal time dealing with the aftereffects of the Data Breach, suggesting that Plaintiff and Class Members "remain vigilant and monitor your account statements, explanation of benefits, and credit bureau reports closely," and to consider placing a fraud alert on their credit reports.[18]

78. Plaintiff and Class Members have been damaged by the compromise of their Private Information in the Ransomware Attack.

79. Plaintiff Lugenia Booker's Private Information, including her Protected Health Information (PHI), was compromised as a direct and proximate result of the Ransomware Attack.

80. As a direct and proximate result of Defendants' conduct, Plaintiff and Class Members have been placed at an imminent, immediate, and continuing increased risk of harm from fraud and identity theft.

81. Plaintiff and Class Members face substantial risk of out of pocket fraud losses such as loans opened in their names, medical services building their names, tax return fraud, utility bills opened in their names, credit card fraud, and similar identity theft.

82. Plaintiff and Class Members face substantial risk of being targeted for future phishing, data intrusion, and other illegal schemes based on their PHI and other Private Information as potential fraudsters could use that information to more effectively target such schemes to Plaintiff and Class Members.

[18] https://ago.vermont.gov/blog/2020/01/28/personal-touch-holding-corp-personal-touch-home-care-of-greater-portsmouth-notice-of-data-breach-to-consumers/

83. Plaintiff and Class Members may also incur out-of-pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Ransomware Attack.

84. Plaintiff and Class Members suffered a loss of value of their Private Information when it was acquired by cyber thieves in the Ransomware Attack. Numerous courts have recognized the propriety of loss of value damages in related cases.

85. Plaintiff and Class Members were also damaged via benefit of the bargain damages. Both overpaid for a service that was intended to be accompanied by adequate data security but was not. Part of the price class members paid to Defendants was intended to be used by Defendants to fund adequate security of Defendants' computer property and Plaintiff's and Class Members' Private Information. Thus, Plaintiff and the class members did not get what they paid for.

86. Plaintiff and Class Members have spent and will continue to spend significant amounts of time to monitor their financial and medical accounts and records for misuse.

87. Plaintiff and Class Members have suffered or will suffer actual injury as a direct result of the Ransomware Attack. In addition to the loss of use of and access to their medical records and costs associated with the inability to access their medical records (including actual disruption of medical care and treatment), many victims suffered ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Ransomware Attack relating to:

a. Finding alternative medical care and treatment;

b. Delaying or foregoing medical care and treatment;

c. Undergoing medical care and treatment without medical providers having access to a complete medical history and records;

d. Having to retrace or recreate their medical history;

e. Finding fraudulent charges;

f. Canceling and reissuing credit and debit cards;

g. Purchasing credit monitoring and identity theft prevention;

h. Addressing their inability to withdraw funds linked to compromised accounts;

i. Taking trips to banks and waiting in line to obtain funds held in limited accounts;

j. Placing "freezes" and "alerts" with credit reporting agencies;

k. Spending time on the phone with or at the financial institution to dispute fraudulent charges;

l. Contacting their financial institutions and closing or modifying financial accounts;

m. Resetting automatic billing and payment instructions from compromised credit and debit cards to new ones;

n. Paying late fees and declined payment fees imposed as a result of failed automatic payments that were tied to compromised cards that had to be cancelled; and

o. Closely reviewing and monitoring bank accounts and credit reports for unauthorized activity for years to come.

88. Moreover, Plaintiff and Class Members have an interest in ensuring that their Private Information, which is believed to remain in the possession of Defendants, is protected from further breaches by the implementation of security measures and safeguards, including but not

limited to, making sure that the storage of data or documents containing personal and financial information is not accessible online and that access to such data is password-protected.

89. Further, as a result of Defendants' conduct, Plaintiff and Class Members are forced to live with the anxiety that their Private Information and medical treatments may be disclosed to the entire world, thereby subjecting them to embarrassment and depriving them of any right to privacy whatsoever.

90. As a direct and proximate result of Defendants' actions and inactions, Plaintiff and Class Members have suffered anxiety, emotional distress, and loss of privacy, and are at an increased risk of future harm.

CLASS ACTION ALLEGATIONS

91. Plaintiff brings this action on behalf of herself and on behalf of all other persons similarly situated ("the Class") pursuant to Rule 23 (b)(2), (b)(3) and (c)(4) of the Federal Rules of Civil Procedure.

92. Plaintiff proposes the following Class definition, subject to amendment as appropriate:

> All persons who utilized Defendant Personal Touch's services and whose Private Information was maintained on Defendant Crossroads' cloud-based electronic health records system that was compromised in the Ransomware Attack, and who were sent notice of the Data Breach.

Excluded from the Class are Defendant's officers, directors, and employees; any entity in which Defendants have a controlling interest; and the affiliates, legal representatives, attorneys, successors, heirs, and assigns of Defendants. Excluded also from the Class are Members of the judiciary to whom this case is assigned, their families and Members of their staff.

93. Numerosity. The Members of the Class are so numerous that joinder of all of them is impracticable. While the exact number of Class Members is unknown to Plaintiff at this time,

based on information and belief, the Class consists of approximately 156,409 patients of Defendant Personal Touch whose data was compromised in the Ransomware Attack.

94. Commonality. There are questions of law and fact common to the Class, which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

a. Whether Defendants unlawfully used, maintained, lost, or disclosed Plaintiff's and Class Members' Private Information;

b. Whether Defendants failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Ransomware Attack;

c. Whether Defendants' data security systems prior to and during the Data Breach complied with applicable data security laws and regulations including, e.g., HIPAA;

d. Whether Defendants' data security systems prior to and during the Data Breach were consistent with industry standards;

e. Whether Defendants owed a duty to Class Members to safeguard their Private Information;

f. Whether Defendants breached their duty to Class Members to safeguard their Private Information;

g. Whether computer hackers obtained Class Members' Private Information in the Ransomware Attack;

h. Whether Defendants knew or should have known that its data security systems and monitoring processes were deficient;

i. Whether Plaintiff and Class Members suffered legally cognizable damages as a result of Defendants' misconduct;

j. Whether Defendants' conduct was negligent;

k. Whether Defendants' conduct was *per se* negligent;

l. Whether Defendants' acts, inactions, and practices complained of herein amount to acts of intrusion upon seclusion under the law;

m. Whether Defendants failed to provide notice of the Ransomware Attack in a timely manner, and;

n. Whether Plaintiff and Class Members are entitled to damages, civil penalties, punitive damages, and/or injunctive relief.

95. Typicality. Plaintiff's claims are typical of those of other Class Members because Plaintiff's information, like that of every other Class member, was compromised in the Ransomware Attack.

96. Adequacy of Representation. Plaintiff will fairly and adequately represent and protect the interests of the Members of the Class. Plaintiff's Counsel are competent and experienced in litigating Class actions.

97. Predominance. Defendants have engaged in a common course of conduct toward Plaintiff and Class Members, in that all the Plaintiff's and Class Members' data was stored on the same computer systems and unlawfully accessed in the same way. The common issues arising from Defendants' conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

98. Superiority. A Class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a Class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Defendants. In contrast, the conduct of this action as a Class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class member.

99. Defendants have acted on grounds that apply generally to the Class as a whole, so that Class certification, injunctive relief, and corresponding declaratory relief are appropriate on a Class-wide basis.

CAUSES OF ACTION

FIRST COUNT
Negligence
(On Behalf of Plaintiff and All Class Members)

100. Plaintiff re-alleges and incorporates by reference Paragraphs 1 through 99 above as if fully set forth herein.

101. Defendant Personal Touch required Plaintiff and Class Members to submit non-public personal information in order to obtain medical services.

102. By collecting and storing this data in Crossroads' computer property, and sharing it and using it for commercial gain, Defendants had a duty of care to use reasonable means to secure and safeguard their computer property—and Class Members' Private Information held

within it—to prevent disclosure of the information, and to safeguard the information from theft. Defendants' duty included a responsibility to implement processes by which they could detect a breach of their security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a ransomware attack.

103. Defendants owed a duty of care to Plaintiff and Class Members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that their systems and networks, and the personnel responsible for them, adequately protected the Private Information.

104. Defendants' duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendant Personal Touch and its client patients, which is recognized by laws and regulations including but not limited to HIPAA, as well as common law. Defendants were in a position to ensure that their systems were sufficient to protect against the foreseeable risk of harm to Class Members from a ransomware attack or data breach.

105. Defendants' duty to use reasonable security measures under HIPAA required Defendants to "reasonably protect" confidential data from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 45 C.F.R. § 164.530(c)(1). Some or all of the medical information at issue in this case constitutes "protected health information" within the meaning of HIPAA.

106. In addition, Defendants had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

107. Defendants' duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendants are bound by industry standards to protect confidential Private Information.

108. Defendants breached their duties, and thus were negligent, by failing to use reasonable measures to protect Class Members' Private Information. The specific negligent acts and omissions committed by Defendants include, but are not limited to, the following:

109. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' Private Information;

110. Failing to adequately monitor the security of their networks and systems;

111. Failure to periodically ensure that their email system had plans in place to maintain reasonable data security safeguards;

112. Allowing unauthorized access to Class Members' Private Information;

113. Failing to detect in a timely manner that Class Members' Private Information had been compromised; and

114. Failing to timely notify Class Members about the Ransomware Attack so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

115. It was foreseeable that Defendants' failure to use reasonable measures to protect Class Members' Private Information would result in injury to Class Members. Further, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches in the medical industry.

116. It was therefore foreseeable that the failure to adequately safeguard Class Members' Private Information would result in one or more types of injuries to Class Members.

117. Plaintiff and Class Members are entitled to compensatory and consequential damages suffered as a result of the Ransomware Attack.

118. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendants to (i) strengthen their data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) continue to provide adequate credit monitoring to all Class Members.

SECOND COUNT
Intrusion into Private Affairs / Invasion of Privacy
(On Behalf of Plaintiff and All Class Members)

119. Plaintiff repeats and re-alleges each and every allegation contained in Paragraphs 1 through 99 as if fully set forth herein.

120. The Commonwealth of Pennsylvania recognizes the tort of Intrusion into Private Affairs, and adopts the formulation of that tort found in the Restatement (Second) of Torts, which states:

> One who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person.

Restatement (Second) of Torts § 652B (1977), *see Vogel v. W.T. Grant Co.*, 458 Pa. 124, 327 A.2d 133 (1974).

121. Plaintiff and Class Members had a reasonable expectation of privacy in the Private Information Defendants mishandled. In failing to protect Plaintiff's and Class Members' Private Information, and in intentionally misusing and/or disclosing their Private Information, Defendants acted with intentional malice and oppression and in conscious disregard of Plaintiff's and Class Members' rights to have such information kept confidential and private. Plaintiff, therefore, seeks an award of damages on behalf of herself and the Class.

THIRD COUNT
Breach of Express Contract
(On Behalf of Plaintiff and All Class Members)

122. Plaintiff re-alleges and incorporates by reference Paragraphs 1 through 99 above as if fully set forth herein.

123. Plaintiff and Class Members allege that they entered into valid and enforceable express contracts, or were express, foreseeable, and intended third party beneficiaries, of valid and enforceable express contracts with both Defendants.

124. As the persons whose sensitive Personal Information was being stored by Defendant Crossroads, Plaintiff and Class Members are and were the intended and foreseeable third-party beneficiaries of the contract(s) between Defendant Personal Touch and Defendant Crossroads, contract(s) which (upon information and belief) include obligations to keep sensitive Personal Information (including without limitation HIPAA protected PII and PHI) private and secure.

125. The valid and enforceable express contracts that Plaintiff and Class Members entered into with Defendants include Defendants' promise to protect nonpublic personal information given to Defendant Personal Touch or that Defendant Personal Touch gathers on its own from disclosure.

126. Under these express contracts, Defendants and/or affiliated healthcare providers, promised and were obligated to: (a) provide healthcare to Plaintiff and Class Members; and (b) protect Plaintiff 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, Plaintiff and Class Members agreed to pay money for these services, and to turn over their Private Information.

127. Both the provision of healthcare and the protection of Plaintiff's and Class Members' PII/PHI were material aspects of these contracts.

128. At all relevant times, Defendant Personal Touch expressly represented in Defendant Personal Touch's Privacy Policy that it would, among other things: (A) protect patients' medical information; (B) keep medical information private; (C) give notice of Defendants' legal duties and privacy practices with respect to medical information about patients, (D) follow the terms of the privacy notice that is currently in effect; (E) to make any other uses and disclosures of medical information not covered by the Privacy Notice or the laws that apply to use only with written permission, and; F) notify patients in the event of a breach of unsecured medical information.[19]

129. Defendants' express representations, including, but not limited to, express representations found in the Personal Touch Notice of Privacy Practices, formed an express contract requiring both Defendants to implement data security adequate to safeguard and protect the privacy of Plaintiff's and Class Members' PII/PHI.

130. 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 Plaintiff 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. Plaintiff and Class Members would not have entered into these contracts with Defendants and/or Personal Touch's affiliated medical care providers as a direct or third-party beneficiary without an understanding that their PII/PHI would be safeguarded and protected.

[19] https://www.pthomecare.com/privacy-practices

131. A meeting of the minds occurred, as Plaintiff and Class Members provided their PII/PHI to Defendants and/or Personal Touch's affiliated medical care providers, and paid for the provided healthcare in exchange for, amongst other things, protection of their PII/PHI.

132. Plaintiff and Class Members performed their obligations under the contract when they paid for their health care services and provided their PII/PHI.

133. Defendants materially breached their contractual obligation to protect the nonpublic personal information Defendants gathered when the information was accessed and exfiltrated by unauthorized personnel as part of the Ransomware Attack.

134. Defendants materially breached the terms of these express contracts, including, but not limited to, the terms stated in the relevant Notice of Privacy Practices. Defendants did not maintain the privacy of Plaintiff's and Class Members' PII/PHI as evidenced by Personal Touch's disclosure of the Ransomware Attack. Specifically, Defendants did not comply with industry standards, or otherwise protect Plaintiff's and the Class Members' PII/PHI, as set forth above.

135. The Ransomware Attack was a reasonably foreseeable consequence of Defendants' actions in breach of these contracts.

136. As a result of Defendants' failure to fulfill the data security protections promised in these contracts, Plaintiff and Class Members 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. Plaintiff 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.

137. Had Defendants disclosed that their data security was inadequate or that they did not adhere to industry-standard security measures, neither the Plaintiff, the Class Members, nor

any reasonable person would have purchased healthcare from Defendant Personal Touch and/or its affiliated healthcare providers.

138. As a direct and proximate result of the Ransomware Attack, Plaintiff and Class Members have been harmed and have suffered, and will continue to suffer, actual damages and injuries, including without limitation the release, disclosure, and publication of their PII/PHI, the loss of control of their PII/PHI, the imminent risk of suffering additional damages in the future, disruption of their medical care and treatment, out-of-pocket expenses, and the loss of the benefit of the bargain they had struck with Defendants.

139. Plaintiff and Class Members are entitled to compensatory and consequential damages suffered as a result of the Ransomware Attack.

FOURTH COUNT
Breach of Implied Contract
(On Behalf of Plaintiff and All Class Members)

140. Plaintiff re-alleges and incorporates by reference Paragraphs 1 through 99 above as if fully set forth herein.

141. When Plaintiff and Class Members provided their Private Information to Defendants Personal Touch in exchange for Defendants' services, they entered into implied contracts with Defendants pursuant to which Defendants agreed to reasonably protect such information.

142. Defendant Personal Touch solicited and invited Class Members to provide their Private Information as part of Defendants' regular business practices. Plaintiff and Class Members accepted Defendants' offers and provided their Private Information to Defendants.

143. In entering into such implied contracts, Plaintiff and Class Members reasonably believed and expected that Defendants' data security practices complied with relevant laws and regulations, including HIPAA, and were consistent with industry standards.

144. Class Members who paid money to Defendants reasonably believed and expected that Defendants would use part of those funds to obtain adequate data security. Defendants failed to do so.

145. Plaintiff and Class Members would not have entrusted their Private Information to Defendants in the absence of the implied contract between them and Defendants to keep their information reasonably secure. Plaintiff and Class Members would not have entrusted their Private Information to Defendants in the absence of their implied promise to monitor their computer systems and networks to ensure that it adopted reasonable data security measures.

146. Plaintiff and Class Members fully and adequately performed their obligations under the implied contracts with Defendants.

147. Defendants breached their implied contracts with Class Members by failing to safeguard and protect their Private Information.

148. As a direct and proximate result of Defendants' breaches of the implied contracts, Class Members sustained damages as alleged herein.

149. Plaintiff and Class Members are entitled to compensatory and consequential damages suffered as a result of the Ransomware Attack.

150. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendants to, e.g., (i) strengthen their data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit monitoring to all Class Members.

FIFTH COUNT
Negligence *Per Se*
(On Behalf of Plaintiff and All Class Members)

151. Plaintiff re-alleges and incorporates by reference Paragraphs 1 through 99 above as if fully set forth herein.

152. Pursuant to section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, Defendants had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' Private Information.

153. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses of failing to use reasonable measures to protect PII.

154. Pursuant to HIPAA, 42 U.S.C. § 1302d, *et seq*., Defendants had a duty to implement reasonable safeguards to protect Plaintiff's and Class Members' Private Information.

155. Pursuant to HIPAA, Defendants had a duty to render the electronic PHI they maintained unusable, unreadable, or indecipherable to unauthorized individuals, as specified in the HIPAA Security Rule by "the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key." See definition of encryption at 45 C.F.R. § 164.304.

156. Pursuant to the Gramm-Leach-Bliley Act, 15 U.S.C. § 6801, Defendants had a duty to protect the security and confidentiality of Plaintiff's and Class Members' Private Information.

157. Defendants breached their duties to Plaintiff and Class Members under the Federal Trade Commission Act, HIPAA, and the Gramm-Leach-Bliley Act by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and

Class Members' Private Information and not complying with applicable industry standards, as described in detail herein.

158. Defendants' failure to comply with applicable laws and regulations constitutes negligence per se.

159. But for Defendants' wrongful and negligent breach of their duties owed to Plaintiff and Class Members, Plaintiff and Class Members would not have been injured.

160. The injury and harm suffered by Plaintiff and Class Members was the reasonably foreseeable result of Defendants' breach of their duties. Defendants knew or should have known that they failing to meet their duties, and that Defendants' breach would cause Plaintiff and Class Members to experience the foreseeable harms associated with the exposure of their Private Information.

161. As a direct and proximate result of Defendants' negligent conduct, Plaintiff and Class Members have suffered injury and are entitled to compensatory, consequential, and punitive damages in an amount to be proven at trial.

SIXTH COUNT
Breach of Fiduciary Duty
(On Behalf of Plaintiff and All Class Members)

162. Plaintiff re-alleges and incorporates by reference Paragraphs 1 through 99 above as if fully set forth herein.

163. In light of the special relationship between Defendant Personal Touch and Plaintiff and Class Members, whereby Defendants became guardians of Plaintiff's and Class Members' Private Information, Defendants became fiduciaries by their undertaking and guardianship of the Private Information, to act primarily for the benefit of Personal Touch's patients, including Plaintiff and Class Members, (1) for the safeguarding of Plaintiff's and Class Members' Private

Information; (2) to timely notify Plaintiff and Class Members of a data breach and disclosure; and (3) maintain complete and accurate records of what patient information (and where) Defendants did and does store.

164. As the agent of Defendant Personal Touch for purposes of storing, maintaining, and safeguarding Plaintiff's and Class Members' PII and PHI, Defendant Personal Touch's fiduciary duty is imputed to Defendant Crossroads.

165. Defendants have a fiduciary duty to act for the benefit of Plaintiff and Class Members upon matters within the scope of Personal Touch's patients' relationship, in particular, to keep secure the Private Information of its patients.

166. Defendants breached their fiduciary duties to Plaintiff and Class Members by failing to diligently discovery, investigate, and give notice of the Ransomware Attack in a reasonable and practicable period of time.

167. Defendants breached their fiduciary duties to Plaintiff and Class Members by failing to encrypt and otherwise protect the integrity of the systems containing Plaintiff's and Class Members' Private Information.

168. Defendants breached their fiduciary duties owed to Plaintiff and Class Members by failing to timely notify and/or warn Plaintiff and Class Members of the Ransomware Attack.

169. Defendants breached their fiduciary duties owed to Plaintiff and Class Members by failing to ensure the confidentiality and integrity of electronic PHI Defendants created, received, maintained, and transmitted, in violation of 45 C.F.R. § 164.306(a)(1).

170. Defendants breached their fiduciary duties owed to Plaintiff and Class Members by failing to implement technical policies and procedures for electronic information systems that

maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights in violation of 45 C.F.R. § 164.312(a)(1).

171. Defendants breached their fiduciary duties owed to Plaintiff and Class Members by failing to implement policies and procedures to prevent, detect, contain, and correct security violations, in violation of 45 C.F.R. § 164.308(a)(1).

172. Defendants breached their fiduciary duties owed to Plaintiff and Class Members by failing to identify and respond to suspected or known security incidents and to mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity in violation of 45 C.F.R. § 164.308(a)(6)(ii).

173. Defendants breached their fiduciary duties owed to Plaintiff and Class Members by failing to protect against any reasonably-anticipated threats or hazards to the security or integrity of electronic PHI in violation of 45 C.F.R. § 164.306(a)(2).

174. Defendants breached their fiduciary duties owed to Plaintiff and Class Members by failing to protect against any reasonably anticipated uses or disclosures of electronic PHI that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 C.F.R. § 164.306(a)(3).

175. Defendants breached their fiduciary duties owed to Plaintiff and Class Members by failing to ensure compliance with the HIPAA security standard rules by their workforces in violation of 45 C.F.R. § 164.306(a)(94).

176. Defendants breached their fiduciary duties owed to Plaintiff and Class Members by impermissibly and improperly using and disclosing PHI that is and remains accessible to unauthorized persons in violation of 45 C.F.R. § 164.502, et seq.

177. Defendants breached their fiduciary duties owed to Plaintiff and Class Members by failing to effectively train all Members of their workforces (including independent contractors) on the policies and procedures with respect to PHI as necessary and appropriate for the Members of their workforces to carry out their functions and to maintain security of PHI in violation of 45 C.F.R. § 164.530(b) and 45 C.F.R. § 164.308(a)(5).

178. Defendants breached their fiduciary duties owed to Plaintiff and Class Members by failing to design, implement, and enforce policies and procedures establishing physical and administrative safeguards to reasonably safeguard PHI, in compliance with 45 C.F.R. § 164.530(c).

179. Defendants breached their fiduciary duties to Plaintiff and Class Members by otherwise failing to safeguard Plaintiff's and Class Members' Private Information.

180. As a direct and proximate result of Defendants' breaches of their fiduciary duties, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the compromise, publication, and/or theft of their Private Information; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their Private Information; (iv) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Ransomware Attack, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (v) the continued risk to their Private Information, which remains in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the Private Information in their continued possession; (vi) future costs in terms of time, effort, and money that will be expended as result of the Ransomware Attack for the

remainder of the lives of Plaintiff and Class Members; and (vii) the diminished value of Defendants' services they received.

181. As a direct and proximate result of Defendants' breaches of their fiduciary duties, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm, and other economic and non-economic losses.

SEVENTH COUNT
Pennsylvania Unfair Trade Practices and Consumer Protection Law
73 Pa. Cons. Stat. §§ 201-2 & 201-3, *et seq*.
(On behalf of Plaintiff and all Class Members)

182. Plaintiff re-alleges and incorporates by reference Paragraphs 1 through 99 above as if fully set forth herein.

183. Defendants are each a "person", as meant by 73 Pa. Cons. Stat. § 201-2(2).

184. Plaintiff and Class Members purchased goods and services in "trade" and "commerce," as meant by 73 Pa. Cons. Stat. § 201-2(3), primarily for personal, family, and/or household purposes.

185. Defendants engaged in unfair methods of competition and unfair or deceptive acts or practices in the conduct of their trade and commerce in violation of 73 Pa. Cons. Stat. Ann. § 201-3, including, but not limited to, the following:

a. Representing that their goods and services have characteristics, uses, benefits, and qualities that they do not have (73 Pa. Stat. Ann. § 201-2(4)(v));

b. Representing that their goods and services are of a particular standard or quality if they are another (73 Pa. Stat. Ann. § 201- 2(4)(vii)); and

c. Advertising their goods and services with intent not to sell them as advertised (73 Pa. Stat. Ann. § 201-2(4)(ix)).

186. Defendants' unfair or deceptive acts and practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's and Class Members' Personal and Private Information, which was a direct and proximate cause of the Ransomware Attack;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Ransomware Attack;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Class Members' Personal and Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1302d, *et seq*., and the Gramm-Leach-Bliley Act, 15 U.S.C. § 6801;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff's and Class Members' Personal Information and PHI, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Class members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1302d, *et seq*., and the Gramm-Leach-Bliley Act, 15 U.S.C. § 6801;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff's and Class Members' Personal Information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Class Members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1302d, *et seq*., and the Gramm-Leach-Bliley Act, 15 U.S.C. § 6801.

187. Defendants' representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendants' data security and ability to protect the confidentiality of consumers' Personal Information.

188. Defendants intended to mislead Plaintiff and Class Members and induce them to rely on its misrepresentations and omissions.

189. Had Defendants disclosed to Plaintiff and Class Members that their data systems were not secure and thus vulnerable to attack, Defendants would have been unable to continue in business and they would have been forced to adopt reasonable data security measures and comply with the law. Instead, Defendants held themselves out as secure and were trusted with sensitive and valuable Personal Information regarding thousands of consumers, including Plaintiff and the Class Members.

190. Defendants accepted the responsibility of each being a "steward of data" while keeping the inadequate state of their security controls secret from the public.

191. Plaintiff and the Class Members acted reasonably in relying on Defendants' misrepresentations and omissions, the truth of which they could not have discovered.

192. Defendants acted intentionally, knowingly, and maliciously to violate the Pennsylvania Unfair Trade Practices and Consumer Protection Law, and recklessly disregarded

Plaintiff's and Class Members' rights. Past data breaches and ransomware attacks in the healthcare industry put Defendants on notice that their security and privacy protections were inadequate.

193. As a direct and proximate result of Defendants' unfair methods of competition and unfair or deceptive acts or practices and Plaintiff's and the Class Members' reliance on them, Plaintiff and Class Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from disruption of medical care and treatment; fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Personal and Private Information.

194. Plaintiff and the Class Members seek all monetary and non-monetary relief allowed by law, including actual damages or statutory damages of $100 (whichever is greater), treble damages, attorneys' fees and costs, and any additional relief the Court deems necessary or proper.

EIGHTH COUNT
Breach of Physician-Patient Confidentiality
(On behalf of Plaintiff and all Class Members)

195. Plaintiff re-alleges and incorporates by reference Paragraphs 1 through 99 above as if fully set forth herein.

196. A breach of physician-patient confidentiality is a cognizable cause of action in the Commonwealth of Pennsylvania. *Burger v. Blair Med. Assocs., Inc*., 2007 PA Super 164, ¶ 22, 928 A.2d 246, 251 (2007), aff'd, 600 Pa. 194, 964 A.2d 374 (2009).

197. At all times during Plaintiff's and Class Members' interactions with Defendant Personal Touch, it was fully aware of the confidential and sensitive nature of Plaintiff's and Class Members' PII/PHI that Plaintiff and Class Members provided to Defendant Personal Touch.

198. As alleged herein and above, Defendant Personal Touch's physician-patient relationship with Plaintiff and Class Members was governed by terms and expectations that Plaintiff's and Class Members' PII/PHI would be collected, stored, and protected in confidence, and would not be disclosed to unauthorized third parties.

199. Plaintiff and Class Members provided their PII/PHI to Defendant Personal Touch with the explicit and implicit understanding that Defendant Personal Touch, and all of its agents, would protect and not permit their PII/PHI to be disseminated to any unauthorized parties.

200. Plaintiff and Class Members also provided their PII/PHI to Defendant with the explicit and implicit understanding that Defendant, and all of its agents, would take precautions to protect their PII/PHI from unauthorized disclosure, including precautions such as following basic principles of information security practices.

201. Defendant Personal Touch voluntarily received in confidence Plaintiff's and Class Members' PII/PHI with the understanding that the PII/PHI would not be disclosed or disseminated to the public or any unauthorized third parties.

202. Defendant Personal Touch voluntarily gave and entrusted the Plaintiff's and Class Members' PII/PHI to its agent, Defendant Crossroads, with the understanding that the PII/PHI would not be disclosed or disseminated to the public or any unauthorized third parties.

203. As Personal Touch's authorized agent, Defendant Crossroads assumed the duty of confidence that Defendant Personal Touch owed to Plaintiff and Class Members.

204. Due to Defendant Crossroads' failure to prevent, detect, or avoid the Ransomware Attack from occurring by, inter alia, following industry standard information security practices to secure Plaintiff's and Class Members' PII/PHI, Plaintiff's and Class Members' PII/PHI was

disclosed and misappropriated to unauthorized third parties beyond Plaintiff's and Class Members' confidence, and without their express permission.

205. As a direct and proximate cause of Defendants' actions and/or omissions, Plaintiff and Class Members have suffered damages.

206. But for Defendants' disclosure of Plaintiff's and Class Members' PII/PHI in violation of the parties' understanding of confidence, their PII/PHI would not have been compromised, stolen, viewed, accessed, and used by unauthorized third parties. Defendants' acts or omissions in permitting the Ransomware Attack were the direct and legal cause of the theft of Plaintiff's and Class Members PII/PHI, as well as the resulting damages.

207. The injury and harm Plaintiff and Class Members suffered was the reasonably foreseeable result of Defendants' unauthorized disclosure of Plaintiff's and Class Members' PII/PHI.

208. As a direct and proximate result of the Ransomware Attack, Plaintiff and Class Members have been harmed and have suffered, and will continue to suffer, actual damages and injuries, including without limitation the release, disclosure, and publication of their PII/PHI, the loss of control of their PII/PHI, the imminent risk of suffering additional damages in the future, disruption of their medical care and treatment, out-of-pocket expenses, and the loss of the benefit of the bargain they had struck with Defendants.

209. As a direct and proximate result of Defendants' breach, Plaintiff and Class Members have suffered and will continue to suffer from other forms of injury and/or harm, including but not limited to anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff prays for judgment as follows:

a) For an Order certifying this action as a class action and appointing Plaintiff and her Counsel to represent the Class;

b) For equitable relief enjoining Defendants from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff and Class Members' Private Information, and from refusing to issue prompt, complete and accurate disclosures to Plaintiff and Class members;

c) For equitable relief compelling Defendants to utilize appropriate methods and policies with respect to consumer data collection, storage, and safety, and to disclose with specificity the type of PII and PHI compromised during the Ransomware Attack;

d) For equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendants' wrongful conduct;

e) Ordering Defendants to pay for not less than three years of credit monitoring services for Plaintiff and the Class;

f) For an award of actual damages, compensatory damages, statutory damages, and statutory penalties, in an amount to be determined, as allowable by law;

g) For an award of punitive damages, as allowable by law;

h) For an award of attorneys' fees and costs, and any other expense, including expert witness fees;

i) Pre- and post-judgment interest on any amounts awarded; and

j) Such other and further relief as this court may deem just and proper.

JURY TRIAL DEMAND

Plaintiff demands a jury trial on all issues so triable.

Dated: April 6, 2020

Respectfully submitted,

/s/ Charles E. Schaffer
Charles E. Schaffer
David C. Magagna, Jr.
LEVIN, SEDRAN & BERMAN, LLP
510 Walnut Street, Suite 500
Philadelphia, PA 19106
Tel: (215) 592-1500
Fax: (215) 592-4663
cschaffer@lfsblaw.com
dmagagna@lfsblaw.com

MASON LIETZ & KLINGER LLP
Gary E. Mason (*pro hac vice forthcoming*)
David K. Lietz (*pro hac vice forthcoming*)
5101 Wisconsin Ave., NW, Ste. 305
Washington, DC 20016
Phone: 202.640.1160
gmason@masonllp.com
dlietz@masonllp.com

Gary M. Klinger (*pro hac vice forthcoming*)
MASON LIETZ & KLINGER LLP
227 W. Monroe Street, Suite 2100
Chicago, IL 60630
Tel.: (312) 283-3814
gklinger@masonllp.com

Attorneys for Plaintiff and
the Proposed Class