FILED
2019 Dec-23 PM 02:15
U.S. DISTRICT COURT
N.D. OF ALABAMA

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ALABAMA
WESTERN DIVISION

GERALDINE DANIELS,	)
SHENEKA FRIESON on behalf of	)
GABRYELLA MCCRAW, A MINOR,	)
KIMBERLY TURNER, and	)
MARY WILLIAMS, INDIVIDUALLY	)
AND ON BEHALF OF ALL OTHERS	)
SIMILARLY SITUATED,	)
	)
PLAINTIFFS,	)
	)
v.	)
	)
DCH HEALTHCARE AUTHORITY,	)
d/b/a DCH HEALTH SYSTEM,	)
	)
DEFENDANT.	)

CLASS ACTION COMPLAINT

1. Plaintiffs, GERALDINE DANIELS, SHENEKA FRIESON on behalf of GABRYELLA MCCRAW, A MINOR, KIMBERLY TURNER, and MARY WILLIAMS, individually, and on behalf of all others similarly situated, bring this action against Defendant, DCH HEALTHCARE AUTHORITY d/b/a DCH HEALTH SYSTEM, ("DCH" or "Defendant") to obtain damages, restitution, and injunctive relief for the Class, as defined below, from Defendant. Plaintiffs make the following allegations upon information and belief, except as to their own actions, the investigation of their counsel, and the facts that are a matter of public record:

JURISDICTION AND VENUE

2. The Court has federal question subject matter jurisdiction over this action pursuant to 28 U.S.C. § 1331 because the case features claims that necessarily raise substantial disputed federal issues under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"),

the Federal Trade Commission Act (15 U.S.C. § 45) and the Gramm-Leach-Bliley Act (15 U.S.C. § 6801).

3. Jurisdiction is proper in this Court because the principal place of business for the Defendant is in Tuscaloosa, County, Alabama and because the conduct at issue in this case occurred in Alabama.

4. Venue is proper in this Court as a substantial portion of the acts and transactions that constitute violations of law complained of herein occurred in this District and Defendant conducts substantial business throughout this District.

NATURE OF THE ACTION

5. This class action arises out of the recent ransomware attack at DCH's medical facilities that disrupted operations by, among other things, blocking access to DCH's computer systems and data, including the highly sensitive patient medical records of approximately 32,000 (or more) patients (the "Ransomware Attack"). As a result of the Ransomware Attack, Plaintiffs and class members 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 attack. In addition, Plaintiffs' and class members' sensitive personal information—which was entrusted to DCH, its officials and agents—was compromised and disclosed due to the Ransomware Attack. Information compromised in the Ransomware Attack includes Social Security numbers, health insurance information, medical information, other protected health information as defined by the HIPAA, and additional personally identifiable information ("PII") and protected health information ("PHI") that Defendant collected and maintained (collectively the "Private Information").

6. Plaintiffs bring this class action lawsuit on behalf of those similarly situated to address Defendant's inadequate safeguarding of class members' Private Information that

Defendant collected and maintained, and for failing to provide timely and adequate notice to Plaintiffs 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.

7. Defendant maintained the Private Information in a reckless manner. In particular, the Private Information was maintained on Defendant's computer network in a condition vulnerable to cyberattacks of the type that cause actual disruption to Plaintiffs' and class members' medical care and treatment. As a result of the Ransomware Attack, Plaintiffs' 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 Plaintiffs' and class members' Private Information was a known risk to Defendant, and thus Defendant was on notice that failing to take steps necessary to secure the Private Information from those risks left that property in a dangerous condition.

8. In addition, DCH and its employees failed to properly monitor the computer network and systems that housed the Private Information. Had DCH properly monitored its property, it would have discovered the intrusion sooner.

9. Because of the Ransomware Attack, Plaintiffs 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 Plaintiffs and class members, Plaintiffs and the class members had to forego medical care and treatment or had to seek alternative care and treatment.

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

11. 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.

12. As a result of the Ransomware Attack, Plaintiffs and class members have been exposed to a heightened and imminent risk of fraud and identity theft. Plaintiffs and class members must now and in the future closely monitor their financial accounts to guard against identity theft.

13. Plaintiffs 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.

14. By their Complaint, Plaintiffs seek to remedy these harms on behalf of themselves and all similarly-situated individuals whose Private Information was accessed or ransomed during the Ransomware Attack.

15. Plaintiffs seek remedies including but not limited to compensatory damages, reimbursement of out-of-pocket costs, and injunctive relief including improvements to Defendant's data security systems, future annual audits, and adequate credit monitoring services funded by Defendant.

16. Accordingly, Plaintiffs bring this action against Defendant DCH seeking redress for DCH's unlawful conduct, and asserting claims for: (i) negligence, (ii) an intrusion upon

seclusion, (iii) negligence per se, (iv) breach of express contract, (v) breach of implied contract, and, (vi) breach of fiduciary duty.

PARTIES

17. Plaintiff, GERALDINE DANIELS, is and at all times mentioned herein was an individual citizen of the State of Alabama residing in the City of Livingston.

18. Plaintiff SHENEKA FRIESON, on behalf of GABRYELLA MCCRAW, A MINOR, is and at all times mentioned herein was an individual citizen of the State of Alabama residing in the City of Tuscaloosa. Plaintiff Frieson has legal custody of the minor GABRYELLA MCCRAW, who also is an individual citizen of the State of Alabama residing in the City of Tuscaloosa at the same address as Plaintiff Frieson.

19. Plaintiff, KIMBERLY TURNER, is and at all times mentioned herein was an individual citizen of the State of Alabama residing in the City of Butler.

20. Plaintiff, MARY WILLIAMS, is and at all times mentioned herein was an individual citizen of the State of Alabama residing in the City of Greensboro.

21. Defendant DCH is an Alabama "health care authority" within the meaning of the Health Care Authorities (HCA) Act (Ala. Code 1975 § 22-21-318 et seq.) with its principal place of business in Tuscaloosa, Alabama. Defendant has the capacity to be sued pursuant to Ala. Code 1975 § 22-21-318(a)(2), and is not entitled to sovereign immunity under Art. I, § 14, Ala. Const. 1901.

22. Defendant DCH operates three (3) hospitals in West Alabama. The three hospitals are as follows:

A. DCH Regional Medical Center in Tuscaloosa, Alabama;

B. Northport Medical Center in Northport, Alabama;

C. Fayette Medical Center in Fayette, Alabama.

In addition, Defendant also operates the Fayette Long-Term Care Facility in Fayette, Alabama.

DEFENDANT'S BUSINESS

23. Defendant is in the business of rendering hospital and healthcare services at the three hospitals and the long-term care facility listed in Paragraph 22 of this Complaint.

24. Defendant provides comprehensive medical care to patients from across the State of Alabama and from around the country.

25. Services and subspecialties offered by Defendant include, but are not limited to, the following: specialty units for pediatrics, orthopedics, cancer and cardiology, as well as the region's most advanced trauma center and intensive care units, a Bloodless Medicine and Surgery program, microsurgery, laser surgery, laparoscopic and robotic surgery, the Diabetes Education Center, home care services, home medical equipment, occupational medicine, palliative care, physical rehabilitation, sleep services, spine care, sports medicine, women's services, and wound healing.

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

- Name, address, phone number and email address;
- Social Security number;
- Information relating to individual medical history;
- Insurance information and coverage;
- Information concerning an individual's doctor, nurse or other medical providers; and
- Other information that may be deemed necessary to provide care.

27. Defendant also gathers certain medical information about patients and creates records of the care they provide to them.

28. Additionally, Defendant may receive private and personal information from other individuals and/or organizations that are part of a patient's "circle of care", such as referring physicians, patients' other doctors, patient's health plan(s), close friends, and/or family members.

29. All of Defendant's employees, staff, entities, clinics, sites, and locations may share patient information with each other for various purposes, as disclosed in the DCH Health System Notice of Privacy Practices (the "Privacy Notice").[1] The current privacy notice has an effective date of May 1, 2014.

30. The Privacy Notice is provided to every patient upon request.

31. Because of the highly sensitive and personal nature of the information Defendant acquire and stores with respect to its patients, DCH promises to: (1) "maintain the privacy and security of your protected health information"; (2) let a patient "know promptly if a breach occurs that may have compromised the privacy or security of your information"; (3) "follow the duties and privacy practices described in this notice and give you a copy of it," and; (4) "not use or share your information other than as described here unless you tell us we can in writing."

THE RANSOMWARE ATTACK

32. 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.[2]

[1] https://www.dchsystem.com/sites/www/Uploads/files/Form/privacydoc.pdf
[2] https://www.proofpoint.com/us/threat-reference/ransomware.

33. On October 1, 2019, it was reported the DCH hospitals were temporarily closed due to a ransomware attack that was holding their computer systems, including patient files and medical records, hostage.

34. Because of the Ransomware Attack, the three DCH Regional Medical Centers in Tuscaloosa, Fayette, and Northport closed that morning to everyone except any new patients in critical condition.

35. In addition, ambulances in the regions were directed to other hospitals, outpatients were asked to reschedule appointments, and stabilized patients were to be moved to alternate hospitals.

36. As a consequence of the cyber-attack on DCH's computer systems, the affected data was encrypted and locked away by the ransomware. This data included the Private Information, i.e., medical records, demographics, insurance information, medical history, treatment, and billing information, of Defendant's patients, patients who entrusted Defendant with this highly sensitive and private information.

37. On that same day, October 1, 2019, DCH posted the following notice on its website:

> "The three hospitals of the DCH Health System have experienced a ransomware attack. A criminal is limiting our ability to use our computer systems in exchange for an as-yet unknown payment.
>
> Our hospitals have implemented our emergency procedures to ensure safe and efficient operations in the event technology dependent on computers is not available. That said, we feel it is in the best interest of patient safety that DCH Regional Medical Center, Northport Medical Center and Fayette Medical Center are closed to all but the most critical new patients.
>
> Our staff is caring for the patients who are currently in the hospital, and we have no plans to transfer current patients. If you are scheduled for an outpatient procedure or test at a DCH hospital, call before you come. Local ambulances have been instructed to take patients to other hospitals if at all possible. Patients who

come to our emergency departments may be transferred to another hospital when they are stabilized."[3]

38. On October 2, 2019, DCH posted a follow-up statement on its website:

"Early Oct. 1, the DCH Heath System discovered that it had suffered a ransomware attack that impacted their systems. We immediately implemented emergency procedures to continue providing safe and patient-centered care. While the attack has impacted DCH's ability to accept new patients, we are still able to provide critical medical services to those who need it. Patients who have non-emergency medical needs are encouraged to seek assistance from other providers while DCH works to restore its systems.

Our staff of local doctors and nurses are responding to the community's urgent needs, and the needs of our existing patients in our hospitals. Rest assured, their needs are met and at this time patients are not being transferred.

Some outpatient procedures are still being conducted at the DCH hospitals. If a patient has a scheduled procedure or test at a DCH hospital, they should call prior to confirm the appointment.

DCH is proud to be community owned and staffed by local doctors and nurses. We appreciate everyone's understanding and patience as we work through our emergency procedures to resume normal operations.

We are constantly evaluating our situation, and we will provide updates."[4]

39. On October 2, 2019, DCH also published an FAQ on its website, in which it reported that the ransomware attack occurred on October 1, 2019, and that an unknown individual "used malicious software to encrypt files and restrict access to computer systems serving DCH Regional Medical Center, Northport Medical Center and Fayette Medical Center. Investigators have determined that the ransomware variant Ryuk was used to encrypt the files."[5]

---

[3] https://www.al.com/news/2019/10/dch-health-system-closed-to-all-but-most-critical-new-patients-due-to-ransomware-attack.html

[4] https://www.al.com/news/2019/10/dch-health-system-closed-to-all-but-most-critical-new-patients-due-to-ransomware-attack.html

[5] https://www.dchsystem.com/Articles/patient_and_community_information_regarding_attack_on_dch_computer.aspx

40. The Ryuk ransomware virus was first spotted in August 2018, fourteen months prior to DCH's Ransomware Attack announcement. The cybersecurity firm Crowdstrike believes the Ryuk ransomware attacks emanate from a hacker group in Russia known as "WIZARD SPIDER" and that the Russian group has netted about $3.7 million in bitcoins since August 2018.

41. The news website Security Intelligence reported that computers at more than 100 businesses in the U.S. were infected with the Ryuk virus between August 2018 and May 2019.[6]

42. The United Kingdom (UK) National Cyber Security Centre (NCSC) issued an "emergency alert" advisory on Ryuk attacks globally in June 2019. This advisory was further disseminated by the US Department of Homeland Security.[7]

43. DCH provided additional statements on its website on October 2, 2019, an update on October 3, 2019 at 3:30 p.m., October 5, 2019 at 8:30 a.m., and October 7, 2019 at 2:30 p.m.[8]

44. On or about October 5, 2019, DCH paid the ransom that was demanded in order to obtain an encryption key from the attacker. DCH spokesman Brad Fisher issued a statement saying:

> "We worked with law enforcement and IT security experts to assess all options and execute the solution that was best for our patients. This included purchasing an encryption key from the attacker to expedited system recovery and help ensure patient safety. For ongoing security reasons we will be keeping confidential specific details about the investigation and our coordination with the attacker."[9]

---

[6] https://securityintelligence.com/news/more-than-100-us-businesses-affected-by-ryuk-ransomware-since-august-2018-finds-fbi/

[7] https://www.us-cert.gov/ncas/current-activity/2019/06/28/ncsc-releases-advisory-ryuk-ransomware

[8] https://www.dchsystem.com/Articles/dch_ongoing_response_to_cyberattack_and_it_system_outage.aspx

[9] https://www.wsfa.com/2019/10/02/dch-hospitals-not-taking-new-patients-unless-they-are-critical-due-ransomware-attack/

45. On October 10, 2019, DCH tweeted out a notice that normal operations had resumed, and issued the following statement:

> DCH continues working hard to restore our systems so we can resume normal operations and provide high-quality, patient-centered care to our communities. We have made a major step in this process today. On Thursday, Oct. 10, DCH lifted diversion protocol for its three hospitals and resumed taking patients in its Emergency Departments. All hospital services are open. (See special note about Outpatient Imaging below.)
>
> This comes after a methodical process of system restoration following a cyberattack that disrupted the health system's computer system in the early morning hours of Oct. 1. From Oct. 1 to Oct. 9, DCH hospitals operated under downtime procedures. These are established paper-based charting and ordering procedures that are used when computer systems are off line for maintenance. While operating on downtime procedures, DCH hospitals asked Emergency Medical Services to divert all but the most critical patients to other hospitals. Our Emergency Departments continued to see patients who brought themselves to the hospital. Most elective surgeries and many other procedures were performed as scheduled during the event.
>
> Essential electronic systems related to patient care have been restored, allowing DCH to begin receiving patients. DCH's IT Department continues to restore certain nonessential systems, including the email system, and they are working to fully optimize systems to their speed and functionality before the cyberattack. We do not have a timetable for when all systems will be fully optimized.
>
> We sincerely apologize for the frustration and inconvenience this incident has caused, especially to our patients and dedicated staff. DCH greatly appreciates everyone's continued patience and support.[10]

46. Defendant 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.

[10] https://www.dchsystem.com/Articles/dch_emergency_departments_resume_taking_all_patients_hospital_services_now_open.aspx

47. Plaintiffs and class members provided their Private Information to Defendant with the reasonable expectation and mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access.

48. Defendant's 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. The increase in such attacks, and attendant risk of future attacks, was widely known to the public and to anyone in Defendant's industry, including Defendant DCH.

49. Defendant breached its obligations to Plaintiffs and class members and/or was otherwise negligent and reckless because it failing to properly maintain and safeguard its computer systems and data. Defendant's 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 protecting patients' Private Information;

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

d. Failing to ensure that its vendors with access to its computer systems and data employed reasonable security procedures;

e. Failing to ensure the confidentiality and integrity of electronic protected health information ("PHI") they 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. 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 its workforces in violation of 45 C.F.R. § 164.306(a)(4);

l. Failing to train all members of its workforces effectively on the policies and procedures regarding PHI as necessary and appropriate for the members of its 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

employees who opened files containing the Ryuk virus, Defendant negligently and unlawfully failed to safeguard consumers' Private Information.

51. Accordingly, as outlined below, Plaintiffs' and class members' 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 at medical facilities such as Defendant's are incredibly 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 breach incident, the death rate among patients increased in the months and years after the attack.[11]

56. Researchers have further found that at medical facilities that experienced a data breach incident, the breach incident was associated with deterioration in timeliness and patient outcomes generally.[12]

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

[11] *See* https://www.pbs.org/newshour/science/ransomware-and-other-data-breaches-linked-to-uptick-in-fatal-heart-attacks.
[12] *See* https://onlinelibrary.wiley.com/doi/full/10.1111/1475-6773.13203.

a. reschedule their medical treatment;

b. find alternative medical care and treatment;

c. delay or forego medical care and treatment; and

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

e. who are unable to access their medical records.[13]

58. Ransomware attacks also constitute data breaches in the traditional sense. For example, 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)."[14]

59. Ransomware attacks are also considered a breach under the HIPAA Rules because there was 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[15]

60. Other security experts agree that when ransomware attack occurs, a data breach does as well, because such an attack represents a loss of control of the data within a network.[16]

---

[13] *See, e.g.*, https://nakedsecurity.sophos.com/2019/10/03/ransomware-attacks-paralyze-and-sometimes-crush-hospitals/; https://healthitsecurity.com/news/data-breaches-will-cost-healthcare-4b-in-2019-threats-outpace-tech.

[14] *See* https://www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf.

[15] *Id.*

[16] *See e.g.*, https://www.csoonline.com/article/3385520/how-hackers-use-ransomware-to-hide-data-breaches-and-other-attacks.html; https://www.varonis.com/blog/is-a-ransomware-attack-a-data-breach/; https://digitalguardian.com/blog/ransomware-infection-always-data-breach-yes.

61. 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).[17]

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

63. 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."[18]

64. 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.[19]

---

[17] See https://www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf

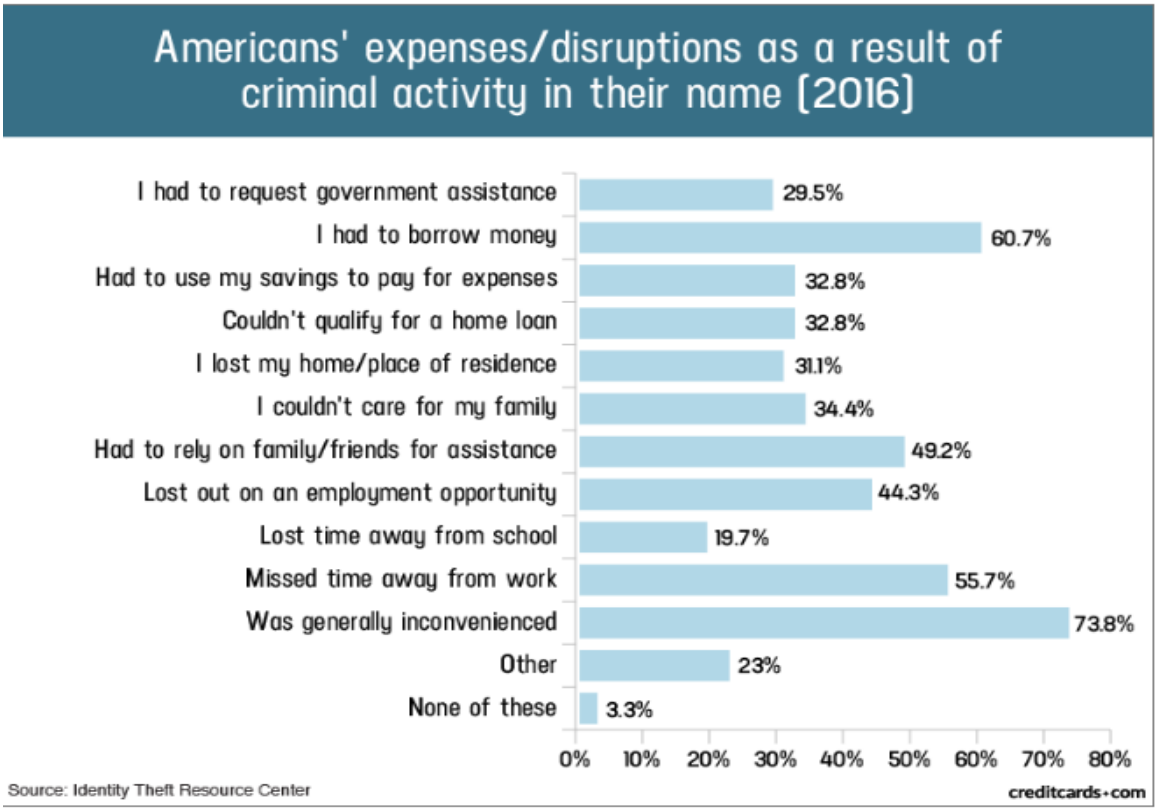
[18] *See* "Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown," p. 2, U.S. Government Accountability Office, June 2007, https://www.gao.gov/new.items/d07737.pdf (last visited Apr. 12, 2019) ("GAO Report").

[19] *See* https://www.identitytheft.gov/Steps (last visited April 12, 2019).

65. 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.

66. 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:[20]

[20] "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).



67. What's more, theft of Private Information is also gravely serious. PII/PHI is a valuable property right.[21] 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.

68. 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

[21] *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."[22] 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.

69. 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.

70. 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.

71. 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 Plaintiffs and Class members are at an increased risk of fraud and identity theft for many years into the future. Thus, Plaintiffs and class members must vigilantly monitor their financial and medical accounts for many years to come.

[22] *See* Federal Trade Commission, Medical Identity Theft, http://www.consumer.ftc.gov/articles/0171-medical-identity-theft (last visited March 27, 2014).

72. 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.[23]

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

PLAINTIFFS' AND CLASS MEMBERS' DAMAGES

74. To date, Defendant has done absolutely nothing to provide Plaintiffs 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 service at Defendants' medical facilities. Nor has Defendant offered any protection against the likely and probable effects that will result from Plaintiffs' and Class Members' Private Information being stolen in connection with the attack. No credit monitoring has been offered. Defendant has not even given any official notice of the Ransomware Attack, instead providing consumers like Plaintiffs with false assurances that their Private Information has not been misused or removed from Defendant's computer system.

75. Plaintiffs and class members have been damaged by the compromise of their Private Information in the Ransomware Attack.

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

76. Plaintiff Geraldine Daniels' medical records were compromised and her medical care disrupted as a direct and proximate result of the Ransomware Attack. Plaintiff Daniels was hospitalized and had surgery at DCH. As a post-surgical patient at DCH, she suffered severe pain and couldn't get the medications that were prescribed to her during her stay for numerous hours after her surgery. During the Ransomware attack, all her medical document files were lost or inaccessible, and everything that was on file was lost or inaccessible during her hospital stay.

77. The medical records of Gabryella McCraw, the minor upon whose behalf Plaintiff Sheneka Frieson is acting, were compromised and her medical care disrupted as a direct and proximate result of the Ransomware Attack. Ms. McCraw is 7 years old, was born at Northport (one of the DCH facilities), and was seen as a patient at Northport 2 to 3 years prior to the Ransomware Attack. On the Saturday following the week of the Ransomware Attack, Plaintiff Frieson took Ms. McCraw to Northport in order to obtain treatment for a severe allergic reaction to something that she ate. The allergic reaction caused both Ms. McCraw's eyes to swell shut and for her to have red marks all over her face. Upon presenting at Northport for treatment, a triage nurse informed Plaintiff Frieson of the Ransomware Attack, told her that part of the ransom had been paid, but that the hospital still could not see patients other than emergency room patients, or that it would be a 4-5 hour wait for treatment. Plaintiff Frieson's options were to drive to Walgreens for medications or to drive to Birmingham for treatment. As a consequence of this disruption to her medical care, it took three days for Ms. McCraw's swelling to go down.

78. Plaintiff Kimberly Turner's medical records were compromised and her medical care disrupted as a direct and proximate result of the Ransomware Attack. Plaintiff Turner was admitted to (and treated in) the DCH Emergency Room on September 27, 2019. While there, she was x-rayed, examined, and told to consult with an orthopedic doctor. The following week, on

October 6, 2019, she saw Dr. Barry Callahan with UO in Tuscaloosa. During the Ransomware attack, all her medical document files were lost or inaccessible, and everything that was on file was lost or inaccessible. As a consequence, she had to have all new x-rays taken and had to basically start over with her care and treatment because her medical records from September 27, 2019 were not available as a result of the Ransomware attack.

79. Similarly, Plaintiff Mary Williams's medical records were compromised and her medical care disrupted as a direct and proximate result of the Ransomware Attack.

80. Like Plaintiffs Daniels, Frieson, Turner, and Williams, as a direct and proximate result of Defendant's conduct, class members had their medical care and treatment disrupted and compromised.

81. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class members have been placed at an imminent, immediate, and continuing increased risk of harm from fraud and identity theft.

82. Plaintiffs 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.

83. Plaintiffs 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 Plaintiffs and class members.

84. Plaintiffs 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.

85. Plaintiffs 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.

86. Class members were also damaged via benefit of the bargain damages. Such class members 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 Defendant was intended to be used by Defendant to fund adequate security of Defendant's computer property and Plaintiffs' and class members' Private Information. Thus, Plaintiffs and the class members did not get what they paid for.

87. Plaintiffs 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.

88. Plaintiffs 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.

89. Moreover, Plaintiffs and Class members have an interest in ensuring that their Private Information, which is believed to remain in the possession of Defendant, 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.

90. Further, as a result of Defendant's conduct, Plaintiffs and Class members are forced to live with the anxiety that their Private Information—which contains the most intimate details

about a person's life, including what ailments they suffer, whether physical or mental—may be disclosed to the entire world, thereby subjecting them to embarrassment and depriving them of any right to privacy whatsoever.

91. As a direct and proximate result of Defendant's actions and inactions, Plaintiffs and Class members have suffered anxiety, emotional distress, and loss of privacy, and are at an increased risk of future harm.

CLASS ACTION ALLEGATIONS

92. Plaintiffs bring this action on behalf of themselves and on behalf of all other persons similarly situated ("the Class").

93. Plaintiffs propose the following Class definition, subject to amendment as appropriate:

> All persons who utilized Defendant's services and whose Private Information was maintained on Defendant's system that was compromised in the Ransomware Attack announced by Defendant on or about October 1, 2019.

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

94. 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 Plaintiffs at this time, based on information and belief, the Class may approach patients.

95. 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 Defendant unlawfully used, maintained, lost, or disclosed Plaintiffs' and Class members' Private Information;

b. Whether Defendant 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 Defendant's data security systems prior to and during the Ransomware Attack complied with applicable data security laws and regulations including, *e.g.*, HIPAA;

d. Whether Defendant's data security systems prior to and during the Ransomware Attack were consistent with industry standards;

e. Whether Defendant owed a duty to class members to safeguard their Private Information;

f. Whether Defendant breached its duty to class members to safeguard their Private Information;

g. Whether computer hackers obtained class members' Private Information in the Ransomware;

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

i. Whether Plaintiffs and class members suffered legally cognizable damages as a result of Defendant's misconduct; and

j. Whether Defendant's conduct was negligent;

k. Whether Defendant's conduct was *per se* negligent;

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

m. Whether Plaintiffs and Class members are entitled to damages, treble damages, civil penalties, punitive damages, and/or injunctive relief.

96. Typicality. Plaintiffs' claims are typical of those of other Class members because Plaintiffs' information, like that of every other Class member, was compromised in the Ransomware Attack.

97. Adequacy of Representation. Plaintiffs will fairly and adequately represent and protect the interests of the members of the Class. Plaintiffs' Counsel are competent and experienced in litigating class actions.

98. Predominance. Defendant has engaged in a common course of conduct toward Plaintiffs and class members. The common issues arising from Defendant's 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.

99. 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 claim 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 Defendant. 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.

100. Defendant has 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 under Fed. R. Civ. P. 23(b)(2).

CAUSES OF ACTION

FIRST COUNT

Negligence
(On Behalf of Plaintiffs and All Class Members)

101. Plaintiffs re-allege and incorporate by reference Paragraphs 1 through 100 above as if fully set forth herein.

102. Defendant required Plaintiffs and class members to submit non-public personal information in order to obtain medical services.

103. By collecting and storing this data in its computer property, and sharing it and using it for commercial gain, Defendant had a duty of care to use reasonable means to secure and safeguard its computer property—and class members' Private Information held within it—to prevent disclosure of the information, and to safeguard the information from theft. Defendant's duty included a responsibility to implement processes by which they could detect a breach of its security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a data breach and/or ransomware attack.

104. Defendant owed a duty of care to Plaintiffs and class members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure

that its systems and networks, and the personnel responsible for them, adequately protected the Private Information.

105. Defendant's duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendant and its client patients, which is recognized by laws and regulations including but not limited to HIPAA, as well as common law. Defendant was 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 and/or data breach.

106. Defendant's duty to use reasonable security measures under HIPAA required Defendant 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.

107. In addition, Defendant 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.

108. Defendant's 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 Defendant is bound by industry standards to protect confidential Private Information.

109. Defendant breached its duties, and thus was negligent, by failing to use reasonable measures to protect class members' Private Information. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard class members' Private Information;

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

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

d. Allowing unauthorized access to class members' Private Information;

e. Failing to detect in a timely manner that class members' Private Information had been compromised; and

f. 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.

110. It was foreseeable that Defendant's 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 ransomware attacks and data breaches in the medical industry.

111. 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.

112. Plaintiffs and class members are entitled to compensatory, consequential, and punitive damages suffered as a result of the Ransomware Attack.

113. Plaintiffs and class members are also entitled to injunctive relief requiring Defendant 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 free credit monitoring to all class members.

SECOND COUNT

Intrusion Upon Seclusion / Invasion of Privacy
(On Behalf of Plaintiffs and All Class Members)

114. Plaintiffs repeat and re-allege each and every factual allegation contained in Paragraphs 1 through 100 as if fully set forth herein.

115. Plaintiffs and Class members had a reasonable expectation of privacy in the Private Information Defendant mishandled.

116. Defendant's conduct as alleged above intruded upon Plaintiffs and the Class members' seclusion under common law.

117. By intentionally failing to keep Plaintiffs and Class members' Private Information safe, and by intentionally misusing and/or disclosing said information to unauthorized parties for unauthorized use, Defendant's intentionally invaded Plaintiffs and Class members' privacy by:

a. Intentionally and substantially intruding into Plaintiffs and Class members' private affairs in a manner that identifies the Plaintiffs and Class members and that would be highly offensive and objectionable to an ordinary person; and

b. Intentionally publicizing private facts about the Plaintiffs and Class members, which is highly offensive and objectionable to an ordinary person; and

c. Intentionally causing anguish or suffering to the Plaintiffs and Class members.

118. Defendant knew that an ordinary person in Plaintiffs or Class members' position would consider Defendant's intentional actions highly offensive and objectionable.

119. Defendant invaded Plaintiffs and Class members' right to privacy and intruded into Plaintiffs and Class members' private affairs by intentionally misusing and/or disclosing their Private Information without their informed, voluntary, affirmative, and clear consent.

120. Defendant intentionally concealed from Plaintiffs and Class members an incident that misused and/or disclosed their Private information without their informed, voluntary, affirmative, and clear consent.

121. As a proximate result of such intentional misuse and disclosures, Plaintiffs and Class members' reasonable expectations of privacy in their Private Information was unduly frustrated and thwarted. Defendants' conduct amounted to a substantial and serious invasion of Plaintiffs and Class members' protected privacy interests causing anguish and suffering such that an ordinary person would consider Defendant's intentional actions or inaction highly offensive and objectionable.

122. In failing to protect Plaintiffs and Class members' Private Information, and in intentionally misusing and/or disclosing their Private Information, Defendant acted with intentional malice and oppression and in conscious disregard of Plaintiffs and Class members' rights to have such information kept confidential and private. Plaintiffs, therefore, seeks an award of damages, including punitive damages, on behalf of themselves and the Class.

THIRD COUNT

Breach of Express Contract
(On Behalf of Plaintiffs and All Class Members)

123. Plaintiffs re-allege and incorporate by reference Paragraphs 1 through 100 above as if fully set forth herein.

124. Plaintiffs and Class members, upon information and belief, entered into express contracts with Defendant that include Defendant's promise to protect nonpublic personal information given to Defendant or that Defendant gathers on its own from disclosure.

125. Plaintiffs and Class members performed their obligations under the contract when they paid for their health care services.

126. Defendant breached its contractual obligation to protect the nonpublic personal information Defendant gathered when the information was accessed by unauthorized personnel as part of the Ransomware Attack.

127. As a direct and proximate result of the breach, Plaintiffs and Class members have been harmed and have suffered, and will continue to suffer, damages and injuries.

FOURTH COUNT

Breach of Implied Contract
(On Behalf of Plaintiffs and All Class Members)

128. Plaintiffs re-allege and incorporate by reference Paragraphs 1 through 100 above as if fully set forth herein.

129. When Plaintiffs and class members provided their Private Information to Defendant in exchange for Defendant's services, they entered into implied contracts with Defendant pursuant to which Defendant agreed to reasonably protect such information.

130. Defendant solicited and invited class members to provide their Private Information as part of Defendant's regular business practices. Plaintiffs and class members accepted Defendant's offers and provided their Private Information to Defendant.

131. In entering into such implied contracts, Plaintiffs and class members reasonably believed and expected that Defendant's data security practices complied with relevant laws and regulations, including HIPAA, and were consistent with industry standards.

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

133. Plaintiffs and class members would not have entrusted their Private Information to Defendant in the absence of the implied contract between them and Defendant to keep the

information reasonably secure. Plaintiffs and class members would not have entrusted their Private Information to Defendant in the absence of their implied promise to monitor their computer systems and networks to ensure that they adopted reasonable data security measures.

134. Plaintiffs and class members fully and adequately performed their obligations under the implied contracts with Defendant.

135. Defendant breached its implied contracts class members by failing to safeguard and protect their Private Information.

136. As a direct and proximate result of Defendant's breaches of the implied contracts, class members sustained damages as alleged herein.

137. Plaintiffs and class members are entitled to compensatory, consequential, and punitive damages suffered as a result of the Ransomware Attack.

138. Plaintiffs and class members are also entitled to injunctive relief requiring Defendant to, e.g., (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide free credit monitoring to all class members.

FIFTH COUNT

Negligence *Per Se*
(On Behalf of Plaintiffs and All Class Members)

139. Plaintiffs re-allege and incorporate by reference Paragraphs 1 through 100 above as if fully set forth herein.

140. Pursuant to the Federal Trade Commission Act (15 U.S.C. § 45), Defendant had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiffs' and Class Members' Private Information.

141. Pursuant to HIPAA (42 U.S.C. § 1302d, et seq.), Defendant had a duty to implement reasonable safeguards to protect Plaintiffs' and Class Members' Private Information.

142. Pursuant to HIPAA, Defendant had a duty to render the electronic PHI it 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" (45 CFR 164.304 definition of encryption).

143. Pursuant to the Gramm-Leach-Bliley Act (15 U.S.C. § 6801), Defendant had a duty to protect the security and confidentiality of Plaintiffs' and Class Members' Private Information.

144. Defendant breached its duties to Plaintiffs and Class Members under the Federal Trade Commission Act, HIPAA, and Gramm- Leach-Bliley Act by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiffs' and Class Members' Private Information.

145. Defendant's failure to comply with applicable laws and regulations constitutes negligence *per se*.

146. But for Defendant's wrongful and negligent breach of its duties owed to Plaintiffs and Class Members, Plaintiffs and Class Members would not have been injured.

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

148. As a direct and proximate result of Defendant's negligent conduct, Plaintiffs 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 Plaintiffs and All Class Members)

149. Plaintiffs re-allege and incorporate by reference Paragraphs 1 through 100 above as if fully set forth herein.

150. In light of the special relationship between Defendant and Plaintiffs and Class Members, whereby Defendant became guardians of Plaintiffs' and Class Members' Private Information, Defendant became a fiduciary created by its undertaking and guardianship of the Private Information, to act primarily for the benefit of its patients, including Plaintiffs and Class Members, (1) for the safeguarding of Plaintiffs and Class Members' Private Information; (2) to timely notify Plaintiffs and Class Members' of a ransomware attack and/or data breach and disclosure; and (3) maintain complete and accurate records of what patient information (and where) Defendant did and does store.

151. Defendant has a fiduciary duty to act for the benefit of Plaintiffs and Class Members upon matters within the scope of its patients' relationship, in particular, to keep secure the Private Information of its patients.

152. Defendant breached its fiduciary duties to Plaintiffs and Class Members by failing to diligently investigate the Ransomware Attack to determine the number of Class Members affected in a reasonable and practicable period of time.

153. Defendant breached its fiduciary duties to Plaintiffs and Class Members by failing to encrypt and otherwise protect the integrity of the systems containing Plaintiffs' and Class Members' Private Information.

154. Defendant breached its fiduciary duties owed to Plaintiffs and Class Members by failing to timely notify and/or warn Plaintiffs and Class Members of the Ransomware Attack.

155. Defendant breached its fiduciary duties owed to Plaintiffs and Class Members by failing to ensure the confidentiality and integrity of electronic protected health information Defendant created, received, maintained, and transmitted, in violation of 45 C.F.R. § 164.306(a)(1).

156. Defendant breached its fiduciary duties owed to Plaintiffs and Class Members by failing to implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights in violation of 45 C.F.R. § 164.312(a)(1).

157. Defendant breached its fiduciary duties owed to Plaintiffs 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).

158. Defendant breached its fiduciary duties owed to Plaintiffs and Class Members by failing to identify and respond to suspected or known security incidents; 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).

159. Defendant breached its fiduciary duties owed to Plaintiffs and Class Members by failing to protect against any reasonably-anticipated threats or hazards to the security or integrity of electronic protected health information in violation of 45 C.F.R. § 164.306(a)(2).

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

161. Defendant breached its fiduciary duties owed to Plaintiffs and Class Members by failing to ensure compliance with the HIPAA security standard rules by its workforce in violation of 45 C.F.R. § 164.306(a)(94).

162. Defendant breached its fiduciary duties owed to Plaintiffs and Class Members by impermissibly and improperly using and disclosing protected health information that is and remains accessible to unauthorized persons in violation of 45 C.F.R. § 164.502, et seq.

163. Defendant breached its fiduciary duties owed to Plaintiffs and Class Members by failing to effectively train all members of its workforce (including independent contractors) on the policies and procedures with respect to protected health information as necessary and appropriate for the members of its workforce to carry out their functions and to maintain security of protected health information in violation of 45 C.F.R. § 164.530(b) and 45 C.F.R. § 164.308(a)(5).

164. Defendant breached its fiduciary duties owed to Plaintiffs and Class Members by failing to design, implement, and enforce policies and procedures establishing physical and administrative safeguards to reasonably safeguard protected health information, in compliance with 45 C.F.R. § 164.530(c).

165. Defendant breached its fiduciary duties to Plaintiffs and Class Members by otherwise failing to safeguard Plaintiffs' and Class Members' Private Information.

166. As a direct and proximate result of Defendant's breaches of its fiduciary duties, Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to: (i)

actual disruption of ongoing medical care and treatment; (ii) actual identity theft; (iii) the loss of the opportunity how their Private Information is used; (iv) the compromise, publication, and/or theft of their Private Information; (v) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their Private Information; (vi) 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; (vii) the continued risk to their Private Information, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect Patient Private Information in its continued possession; (viii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the Private Information compromised as a result of the Ransomware Attack for the remainder of the lives of Plaintiffs and Class Members; and (ix) the diminished value of Defendants' services they received.

167. As a direct and proximate result of Defendant's breaches of its fiduciary duties, Plaintiffs and Class Members have suffered and will continue to suffer other forms of injury and/or harm, and other economic and non-economic losses.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs pray for judgment as follows:

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

b) For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiffs and

Class members' Private Information, and from refusing to issue prompt, complete and accurate disclosures to Plaintiffs and Class members;

c) For equitable relief compelling Defendant 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 Defendant's wrongful conduct;

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

f) Ordering Defendant to disseminate individualized notice of the Ransomware Attack to all Class members;

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

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

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

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

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

JURY TRIAL DEMAND

Plaintiffs demands a jury trial on all issues so triable.

Dated: December 23, 2019

Respectfully submitted,

/s Taylor C. Bartlett
Taylor C. Bartlett
ASB-2365-A51B
W. Lewis Garrison, Jr.
ASB-3591-N74W
Attorneys for Plaintiffs
HENINGER GARRISON DAVIS LLC
2224 First Avenue North
Birmingham, AL 35203
(205) 326-3336 Telephone
(205) 380-8085 Facsimile
Taylor@hgdlawfirm.com

WHITFIELD BRYSON & MASON LLP
Gary E. Mason (*pro hac vice forthcoming*)
5101 Wisconsin Ave., NW, Ste. 305
Washington, DC 20016
Phone: 202.640.1160
Fax: 202.429.2294
gmason@wbmllp.com

KOZONIS & KLINGER, LTD.
Gary M. Klinger (*pro hac vice forthcoming*)
4849 N. Milwaukee Ave., Ste. 300
Chicago, Illinois 60630
Phone: 312.283.3814
Fax: 773.496.8617
gklinger@kozonislaw.com