UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF ILLINOIS

SURFSIDE NON-SURGICAL ORTHOPEDICS, P.A., individually and on behalf of all others similarly situated, Plaintiff, v. ALLSCRIPTS HEALTHCARE SOLUTIONS, INC., Defendant.	Case No. **CLASS ACTION COMPLAINT** **Jury Trial Demanded**

Plaintiff Surfside Non-Surgical Orthopedics, P.A., on behalf of itself and all others similarly situated, brings this Class Action Complaint against Allscripts Healthcare Solutions, Inc. and upon personal knowledge as to itself and its own experiences, its counsel's investigations, and as to all other matters, upon information and belief, alleges as follows:

NATURE OF THE ACTION

1. Plaintiff Surfside Non-Surgical Orthopedics, P.A. (hereinafter alternatively "Plaintiff" or "Orthopedics ") brings this class action against Allscripts Healthcare Solutions, Inc. (hereinafter alternatively "Allscripts" or "Defendant") for failing to secure its systems and data from cyberattacks, including ransomware attacks. Accordingly, on January 18, 2018, Allscripts did suffer a ransomware attack, which prevented Allscripts' clients from conducting their routine and ordinary business.

2. As a result of the ransomware attack experienced by Allscripts and as further described below, Plaintiff could not access its patients' records or electronically prescribe medications, forcing Plaintiff to cancel appointments, thereby causing significant business

interruption and disruption, and lost revenues. Additionally, Plaintiff has expended significant time and effort resolving these issues resulting from the breach, including communicating with patients to reschedule appointments.

PARTIES

3. Plaintiff is located and operates a medical practice in Boynton Beach, Florida.

4. Defendant Allscripts Healthcare Solutions, Inc. is a Delaware corporation with its principle place of business in Chicago, Illinois.

JURISDICTION AND VENUE

5. This Court has jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d). The aggregated claims of the individual class members exceed $5,000,000.00, exclusive of interest and costs, and all conditions are met.

6. This Court has jurisdiction over Allscripts as it maintains its corporate headquarters in this District, and for the following reasons: 1) Allscripts makes decisions regarding overall corporate governance and management in this District, including decisions pertaining to the software that it sells and/or manages and the maintenance of the integrity of its servers i.e. security measures to protect its clients' access to electronic health records ("EHRs"); 2) it is authorized to conduct business throughout the United States, including Illinois; 3) it sells and/or licenses proprietary software throughout Illinois and the United States; and, 4) it advertises in a variety of media throughout the United States, including Illinois. Accordingly, via its business operations throughout the United States, Allscripts intentionally avails itself of the markets within this state to render the exercise of jurisdiction by this Court just and proper.

7. Venue is proper in this District pursuant to 28 U.S.C. § 1391(a)(1) because a substantial part of the events and omissions giving rise to this action occurred in this District and because Allscripts is headquartered in this District.

GENERAL FACTUAL BACKGROUND

8. Allscripts Healthcare Solutions, Inc. (MDRX-NASDAQ) is a publicly-traded, American company that provides physician practices, hospitals, and other healthcare providers with technology for practice management and electronic health records. Allscripts also provides solutions for patient engagement and care coordination, as well as financial and analytics technology. The company has more than 180,000 physician users and has solutions in 2,700 hospitals and 13,000 extended care organizations. [1]

9. Allscripts' products and services are used by 45,000 physician practices; 180,000 physicians; 19,000 post-acute agencies; 2,500 hospitals; 100,000 electronic prescribing physicians; 40,000 in-home clinicians; and 7.2 million patients via the Allscripts patient engagement platform.[2]

10. Allscripts primarily derives its revenues from sales of proprietary software to healthcare organizations, which also serves as the basis for its recurring service contracts related to software support and maintenance, as well as certain transaction-related activities, as further described herein. Allscripts offers a suite of EHRs for hospitals, health systems, and physician and community practices. Each of its EHR offerings delivers a single patient record, workflows, and consolidated analytics. Professional EHR is one such offering. Allscripts' Professional EHR is for small to mid-size physician practices. Modules available with Professional EHRs include

[1] Wikipedia, https://en.wikipedia.org/wiki/Allscripts (last visited Jan. 24, 2018).

[2] Allscripts by the Numbers, http://www.allscripts.com/about-allscripts (last visited Jan. 24, 2018).

Allscripts eRecruit, Allscripts Clinical Performance Reporting, Allscripts Practice Management, Allscripts eChart Courier, and Allscripts iAssist.

11. In addition, Allscripts provides various other client services, including installation services and managed services solutions such as outsourcing, private cloud hosting, and revenue cycle management. For the years ending December 31, 2016 and 2015, revenues totaled $1.5 billion and $1.4 billion, respectively, with gross profit attributable to Allscripts totaling $671 million and $581 million, respectively, and income from operations totaling $60 million and $32 million, respectively[3].

12. Because of its involvement with electronic personal health information ("PHI"), Allscripts is both a "Covered Entity" and a "Business Associate" as defined under the rules and regulations promulgated pursuant to the Health Insurance Portability and Accountability Act of 1996 ("HIPAA").[4] The HIPAA "Security Rule," published in 2003, addresses the requirement that both Covered Entities and Business Associates adopt security procedures to assure the confidentiality, integrity, and availability of personal health care information, or PHI.[5]

13. Allscripts' own "Security Program" mirrors the language of its HIPAA obligations as its website states that: "At Allscripts, we are extremely vigilant when it comes to protecting the confidentiality, integrity, and availability of the sensitive information with which we have been entrusted."[6]

---

[3] Allscripts Form 10-K Annual Report for the fiscal year ended December 2016 at p. 110-112.

[4] Allscripts Enterprise, Information Privacy & Security Policies: HIPPA Privacy Policy, Allscripts (Oct. 27, 2015), https://www.allscripts.com/File%20Library/Privacy%20Policy/Allscripts-HIPAA-privacy-policy-2015.pdf; *see also*, 45 CFR Part 160, 164, Subparts A and C

[5] The Security Rule, https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html (last visited Jan. 25 2018), *emphasis added*.

[6] Allscripts Security Program, https://www.allscripts.com/allscripts-com/security-program (last visited Jan. 25, 2018).

14. Allscripts' website also provides the company's "Security Team Vision": "[T]o protect the security of corporate, employee, client and other confidential information; ensure that it is available for use; build confidence in the integrity of information; foster a culture that values security through promoting security awareness and providing guidance on security expectations and goals."[7]

15. Allscripts was aware, however, that at all times pertinent hereto, that deficiencies in its products and services could result in privacy and security vulnerability or compromises, and failed to take adequate measures to protect against any such event. In its most recent 10-K filing, Allscripts poignantly forecasts what eventually happened here and claims it has devoted substantial resources to address such issues:

> **If our security is breached, we could be subject to liability, and clients could be deterred from using our products and services.**
>
> Our business relies on the secure electronic transmission, storage and hosting of sensitive information, including PHI, financial information and other sensitive information relating to our clients, company and workforce. As a result, we face risk of a deliberate or unintentional incident involving unauthorized access to our computer systems or data that could result in the misappropriation or loss of assets or the disclosure of sensitive information, the corruption of data, or other disruption of our business operations. Similarly, denial-of-service, ransomware or other Internet-based attacks may range from mere vandalism of our electronic systems to systematic theft of sensitive information and intellectual property. We believe that, in recent years, companies in our industry have been targeted by such events with increasing frequency, primarily due to the increasing value of healthcare-related data. We have devoted and continue to devote significant resources to protecting and maintaining the confidentiality of this information, including designing and implementing security and privacy programs and controls, training our workforce and implementing new technology. We have no guarantee that these programs and controls will be adequate to prevent all possible security threats. Any compromise of our electronic systems, including the unauthorized access, use or disclosure of sensitive information or a significant disruption of our computing assets and networks, could adversely affect our reputation or our ability to fulfill contractual obligations, could require us to devote significant financial and other resources to mitigate such problems, and could increase our

[7] *Id.*

> future cyber security costs, including through organizational changes, deploying additional personnel and protection technologies, further training of employees, and engaging third party experts and consultants. Moreover, unauthorized access, use or disclosure of such sensitive information could result in civil or criminal liability or regulatory action, including potential fines and penalties. In addition, any real or perceived compromise of our security or disclosure of sensitive information may deter clients from using or purchasing our products and services in the future, which could materially and adversely impact our financial condition and operating results.
>
> Recently, other companies and government agencies have experienced many high-profile incidents involving data security breaches by entities that transmit and store sensitive information. Lawsuits resulting from these security breaches have sought very significant monetary damages, although many of these suits have yet to be resolved. While we maintain insurance coverage that, subject to policy terms and conditions and subject to a significant self-insured retention, is designed to address certain aspects of security-related risks, such insurance coverage may be insufficient to cover all losses or all types of claims that may arise in our business, and we cannot provide assurance that this coverage will prove to be adequate or will continue to be available on acceptable terms.[8]

Ransomware Threatens Healthcare

16. Ransomware is a subset of malware in which the data on a victim's computer, or network, is locked, typically by encryption, and where payment is demanded as a condition of providing the decryption key to unlock the encrypted data and once again make that data available to the victim.[9] The motive for ransomware attacks is nearly always monetary, and the demanded payment is almost always in some form of crypto-currency, typically Bitcoin.[10]

17. Various forms of ransomware have been used to attack corporate as well as individual user systems since as early as 2013. The Cryptolocker strain of ransomware posed as a Trojan horse (malware contained or incorporated within otherwise legitimate-seeming websites, applications, or attachments to emails or messages). In 2017, the WannaCry ransomware

[8] http://investor.allscripts.com/phoenix.zhtml?c=112727&p=irol-reportsannual (last visited Jan. 25, 2018).
[9] Ransomware, http://searchsecurity.techtarget.com/definition/ransomware (last visited Jan. 24, 2018).
[10] *Id.*

attacked and encrypted more than 300,000 Microsoft Windows systems globally, demanding payment in Bitcoin in exchange for the data decryption key. WannaCry's mode of operation closely follows ransomware's general methodology:

> When executed, the WannaCry malware first checks the "kill switch" domain name; if it is not found, then the ransomware encrypts the computer's data, then attempts to exploit the SMB vulnerability to spread out to random computers on the Internet, and "laterally" to computers on the same network. As with other modern ransomware, the payload displays a message informing the user that files have been encrypted, and demands a payment of around $300 in bitcoin within three days, or $600 within seven days.[11]

18. While the extortionist's payment demand is relatively small (ranging between hundreds of dollars to tens of thousands of dollars), the damage wreaked on enterprise and other users' systems runs in to the hundreds of millions of dollars and more.

19. Unlike a data breach, whose seriousness results from the exfiltration and criminal usage of personally identifiable information or personal health care information, a ransomware attack renders data stored within a computer network or individual computer both unreadable and completely inaccessible to the enterprise or computer user. In the case of a health care products or services provider, the consequences can mean life or death.

20. Accordingly, hospitals and other healthcare related facilities and providers are especially attractive targets for ransomware. While no sensitive or health information is disseminated, the risks to patient treatment, health, and safety are significantly increased because of the serious and even life-threatening consequences presented by even a short-lived interruption of healthcare services. One example of this is Hollywood Presbyterian Medical

[11] WannaCry Ransomware Attack, https://en.wikipedia.org/wiki/WannaCry_ransomware_attack (last visited Jan. 24, 2018).

Center in Los Angeles, who in early 2016 was the victim of a ransomware attack and opted to pay $17,000 in Bitcoin to retrieve the key to unlock its data.[12]

21. Other healthcare goods and services providers are not immune from ransomware attacks. In mid-2017, pharmaceutical giant Merck was the subject of the ransomware strain known as "NotPetya." Merck's business was brought to a virtual halt, and the cost to Merck, as of October 2017, amounted to more than $300 million, including more than $175 million in lost business,[13] with the costs to insurers having been estimated at $275 million.[14]

22. It's been reported that the SamSam strain of ransomware has been in existence since at least as early as March 2016, and at that time represented a new method of attack.[15] The malware is spread through poisoned web links and Java applications.

23. A typical SamSam ransomware note following a successful attack appears below:

[12] Richard Winton, Hollywood Hospital Pays $17,000 in Bitcoin to Hackers; FBI Investigating, The LA Times (Feb. 18, 2016), http://www.latimes.com/business/technology/la-me-ln-hollywood-hospital-bitcoin-20160217-story.html.

[13] Patrick Howell O'Neill, NotPetya Ransomware Cost Merck More than $310 Million, Cyber Scoop (Oct. 27, 2017), https://www.cyberscoop.com/notpetya-ransomware-cost-merck-310-million/

[14] Reuters Staff, Merck Cyber Attack May Cost Insurers $275 Million: Verisk's PCS, Reuters (Oct. 19, 2017), https://www.reuters.com/article/us-merck-co-cyber-insurance/merck-cyber-attack-may-cost-insurers-275-million-verisks-pcs-idUSKBN1CO2NP

[15] Tom Spring, New Server-Side Ransomware Hitting Hospitals, Threat Post (Mar. 29, 2016), https://threatpost.com/new-server-side-ransomware-hitting-hospitals/117059/

Test Decryption

Check our site, You can upload 2 encrypted files and we will decrypt your files as demo.

If you are worry that you don't get your keys after you paid, You can get one key for free on you choise(except important servers), Tell us one of your hostn
Also you can get some single key and if all single BTC taht you paid reached to all keys price you will get all keys
Anyway be sure that you will get all your keys if you paid for them and we don't want damage our reliability
With buying the first key you will find that we are honest.

#Where to buy Bitcoin

We advice you to buy Bitcoin with Cash Deposit or WesternUnion From https://localbitcoins.com/ or https://coincafe.com/buybitcoinswestern.php
Because they don't need any verification and send your Bitcoin quickly.

#deadline

You just have 7 days to send us the BitCoin after 7 days we will remove your private keys and it's impossible to recover your files

24. It was widely known that ransomware attacks were a threat in 2018. Indeed, the first ransomware attack was reported to occur in 1989, and involved a healthcare provider.[16]

The January 2018 SamSam Ransomware Event At Allscripts

25. Beginning on or about January 18, 2018, a strain of ransomware known as "SamSam" attacked, compromised, and crippled Allscripts' data centers in Raleigh and Charlotte, North Carolina, disabling Plaintiff's ability to access and transact with Allscripts' electronic health record system, as well as some e-prescribing system capabilities.[17]

26. Allscripts disclosed that its Professional EHR system had been attacked and infected by the SamSam ransomware, resulting in the encryption of patient health-related information used to conduct Allscripts' business. Allscripts has reported that its Professional

[16] Nate Lord, A History of Ransomware Attacks: The Biggest and Worst Ransomware Attacks of All Time, Digital Guardian (Dec. 7, 2017), https://digitalguardian.com/blog/history-ransomware-attacks-biggest-and-worst-ransomware-attacks-all-time

[17] Robert Abel, Allscript still recovering from SamSam Ransomware Attack, SC Media (Jan. 24, 2018), https://www.scmagazine.com/samsam-ransomware-continues-to-wreak-havoc-on-infrastructure/article/738983/

EHR and Electronic Prescriptions for Controlled Substances cloud-based service were the hardest hit by the ransomware attack.[18]

27. What makes the SamSam attack so pernicious is that by encrypting (and hobbling) key components of Allscripts' network, it also hobbled Allscripts' ability to conduct its business – the Allscripts Professional EHR System – and crippling an undisclosed number of e-prescribing system vulnerabilities.[19] This attack hurt both patients and their healthcare providers using the Allscripts systems in that providers were unable to e-prescribe drugs, and patients were unable to obtain drugs e-prescribed for them by those providers

28. Healthcare industry knowledge and awareness of the widespread issues with SamSam ransomware have been known since at least as early as March 2016.[20] Allscripts disregarded Plaintiff's and Class Members' rights by intentionally, willfully, recklessly, and/or negligently failing to take adequate and reasonable measures to implement, monitor, and audit its data systems, which could have prevented or minimized the effects of the SamSam ransomware attack it experienced in January 2018.

29. Ransomware attacks are 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

[18] Marianne Kolbasuk McGee, Allscripts Ransomware Attack a Reminder of Cloud Risks, BankInfo Security (Jan. 22, 2018), https://www.bankinfosecurity.com/allscripts-ransomware-attack-reminder-cloud-risks-a-10602

[19] Robert Abel, Allscript still recovering from SamSam Ransomware Attack, SC Media (Jan. 24, 2018), https://www.scmagazine.com/samsam-ransomware-continues-to-wreak-havoc-on-infrastructure/article/738983/

[20] Server-side Ransomware SAMSAM Hits Healthcare Industry, Trend Micro (Mar. 31, 2016), https://www.trendmicro.com/vinfo/sg/security/news/cybercrime-and-digital-threats/server-side-ransomware-samsam-hits-healthcare-industry

> 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).[21]

30. The SamSam attack on Allscripts' systems and data is 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. 164.402.[22]

31. As of the filing of this Complaint, Allscripts has not disclosed the full nature and extent of the attack on its systems; however, upon information and belief, the full functionality of its services has not yet been restored.

Plaintiff and the Class Suffered Damages

32. Plaintiff and the Class are purchasing users of Allscripts' Professional EHR and electronic prescription products.

33. In their everyday practice, and as an integral part of their business, Plaintiff and the Class place significant reliance on their ability to access and transact with the products and services provided by Allscripts.

34. As a direct and proximate result of Allscripts' wrongful acts and omissions, Plaintiff and the Class suffered, and continue to suffer, economic damage and other actual harm, including monetary losses arising from significant business interruption and disruption, together with expenses incurred in attempts to mitigate such business interruption and disruption.

---

[21] FACT SHEET: Ransomware and HIPAA, https://www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf (last visited Jan. 25, 2018).

[22] *Id.*

35. As of the date of the filing of this Complaint, Plaintiff and the Class continue to experience significant business interruption and disruption as a direct and proximate result of their inability to: access and transact with Allscripts' products and services; submit electronic prescriptions; and to access any patient records or any of the above modules. Allscripts wanton, willful, and reckless disregard caused a complete and total interruption of service, and further caused Plaintiff and the Class monetary and other damages.

36. Allscripts failed to implement appropriate processes that could have prevented or minimized the effects of the SamSam ransomware attack.

37. Plaintiff acted in reasonable reliance on Allscripts' misrepresentations and omissions regarding the security of its product and services, and would not have purchased Allscripts' products and/or software had they known that Allscripts did not take all necessary precautions to protect itself from cyberattack, including ransomware attacks. Plaintiff and the Class would not have gone through with a purchase had they known that the use of Allscripts' products was accompanied by an unreasonable risk of business disruption, interruption and monetary loss.

CLASS ACTION ALLEGATIONS

38. Plaintiff seeks relief in its individual capacity and as representative of all others who are similarly situated. Pursuant to Fed. R. Civ. P. 23(a) and (b)(2), (b)(3), and (c)(4), Plaintiff seeks certification of a Nationwide class. The national class is initially defined as follows: all Allscripts subscribers residing in the United States who were affected by an interruption of service due to the ransomware attack (the "Nationwide Class").

39. Excluded from the above Class are Allscripts, including any entity in which Allscripts has a controlling interest, is a parent or subsidiary, or which is controlled by Allscripts,

as well as the officers, directors, affiliates, legal representatives, heirs, predecessors, successors, and assigns of Allscripts. Also excluded are the judges and court personnel in this case and any members of their immediate families.

40. Numerosity. Fed. R. Civ. P. 23(a)(1). The members of the Class are so numerous that the joinder of all members is impractical. While the exact number of Class members is unknown to Plaintiff at this time, Allscripts provides data services to 45,000 physician practices and 180,000 physicians.

41. Commonality. Fed. R. Civ. P. 23(a)(2) and (b)(3). 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 Allscripts failed to implement, monitor and audit adequate processes to timely detect, prevent, or mitigate a cyberattack;

b. Whether Allscripts' failures and omissions constitute a breach of contract;

c. Whether Allscripts' failures and omissions constitute negligence, gross negligence, or negligence per se;

d. Whether Allscripts unreasonably placed its clients at risk of having their business interrupted and disrupted as a result of a cyberattack;

e. Whether Allscripts' system was vulnerable to cyberattack by reason of their acts and omissions;

f. Whether Allscripts violated the Illinois Consumer Fraud Act by failing to comply with the HIPPA Security Rule; to wit, by failing to implement reasonable security procedures and practices to protect the integrity and availability of PHI;

g. Whether Allscripts violated the Illinois Deceptive Trade Practices Act by failing to comply with the HIPPA Security Rule; to wit, by failing to implement reasonable security procedures and practices to protect the integrity and availability of PHI

h. Which security procedures and which data-breach notification procedures should Allscripts be required to implement as part of any injunctive relief ordered by the Court;

i. Whether Allscripts has an implied contractual obligation to use reasonable security measures;

j. Whether Allscripts has complied with any implied contractual obligation to use reasonable security measures;

k. What security measures, if any, must be implemented by Allscripts to comply with its implied contractual obligations;

l. What the nature of the relief should be, including equitable relief, to which Plaintiff and the Class members are entitled.

42. All members of the proposed Class are readily ascertainable. Allscripts has access to the addresses and other contact information for members of the Class, which can be used for providing notice to many Class members.

43. Typicality. Fed. R. Civ. P. 23(a)(3). Plaintiff's claims are typical of those of other Class members because Plaintiff was denied access to patient EHR, like every other class member.

44. Adequacy of Representation. Fed. R. Civ. P. 23(a)(4). 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, including privacy litigation.

45. Superiority of Class Action. Fed. R. Civ. P. 23(b)(3). A class action is superior to other available methods for the fair and efficient adjudication of this controversy since joinder of all the members of the Class is impracticable. Furthermore, the adjudication of this controversy through a class action will avoid the possibility of inconsistent and potentially conflicting adjudication of the asserted claims. There will be no difficulty in the management of this action as a class action.

46. Damages for any individual class member are likely insufficient to justify the cost of individual litigation, so that in the absence of class treatment, Allscripts' violations of law inflicting substantial damages in the aggregate would go un-remedied without certification of the Class.

47. Class certification is also appropriate under Fed. R. Civ. P. 23(a) and (b)(2), because Allscripts has acted or has refused to act on grounds generally applicable to the Class, so that final injunctive relief or corresponding declaratory relief is appropriate as to the Class as a whole.

COUNT I - NEGLIGENCE, GROSS NEGLIGENCE, AND NEGLIGENCE *PER SE*

(On Behalf of Plaintiff and the Nationwide Class)

48. Plaintiff repeats and fully incorporates all factual allegations contained in paragraphs 1 through 47 as if fully set forth herein.

49. Allscripts owed a duty to Plaintiff and Class Members to exercise reasonable care to safeguard its systems and data from cyberattack, including ransomware attacks.

50. Allscripts is both a Covered Entity as well as a Business Associate; and as such, has a duty to protect PHI in accordance with the provision of HIPPA.

51. Allscripts breached its duties by failing to implement, monitor, and audit the security of its data and systems, resulting in a ransomware attack that significantly impeded and/or prevented its clients' ability to conduct business.

52. Allscripts violated its duties and its obligations under HIPAA as a Covered Entity and a Business Associate by reason of the infiltration of ransomware into its systems and data.

53. Neither Plaintiff nor the Class contributed to the ransomware attack as described in this Complaint.

54. As a direct and proximate result of Allscripts' conduct, Plaintiffs and the Class suffered damages including, but not limited to, disruption and interruption of its business and everyday provision of services to patients.

55. Allscripts' acts and omissions as alleged herein were willful, wanton, and with reckless disregard for the rights of Plaintiff and the Class.

56. Allscripts' acts and omissions in violating HIPAA constitute negligence per se because it failed to maintain the integrity and availability of PHI.

57. As a result of Allscripts' negligence, gross negligence, and negligence per se, Plaintiffs and the Class suffered damages, including costs incurred as a result of both business interruption and disruption, together with other damages as may be shown at trial.

COUNT II – BREACH OF CONTRACT

(On Behalf of Plaintiff and the Nationwide Class)

58. Plaintiff incorporates the factual allegations contained in Paragraphs 1 through 47 as if fully set forth herein.

59. Allscripts entered into contracts with Plaintiff and the Class.

60. Allscripts agreed to provide its specialized services in a professional and workmanlike manner. Implicit in performing these contractual duties is an obligation to reasonably safeguard its systems and data from cyberattack, including ransomware attacks, which can cause an interruption in the flow of an enterprise's routine and everyday provision of services to its clients.

61. Allscripts breached its contracts with Plaintiff and Class members by failing to reasonably safeguard its systems and data from cyberattack, including ransomware attacks.

62. As a direct and proximate result of Allscripts' contract breaches, Plaintiff and the Class sustained actual losses and damages including, but not limited to, complete interruption and disruption of its business of providing services to patients OR complete denial of service and the corresponding inability to operate their business.

COUNT III – UNJUST ENRICHMENT

(On behalf of Plaintiffs and the Nationwide Class)

63. Plaintiff repeats and incorporates the allegations contained in paragraphs 1 through 47 as if fully set forth herein.

64. Plaintiff and the Class conferred a benefit to Allscripts when it entered into a contractual agreement with Allscripts and provided payment for the sale of its products and services.

65. In exchange for, and in consideration of, Plaintiff and Class members providing payment for Allscripts' products and services, Allscripts was required to, and Plaintiff and the Class expected Allscripts to, implement reasonable security policies and procedures that would have detected, prevented, or mitigated a SamSam ransomware attack.

66. Allscripts states that it devotes "significant resources" to protect PHI, a portion of which is derived from the benefit conferred by the contractual payments made by Plaintiff and the Class to Allscripts.

67. As a result of Allscripts acts and omission as alleged herein, Allscripts has been unjustly enriched to the extent that any portion of such contractual payments comprises spending for adequate security not provided.

COUNT IV – VIOLATION OF ILLINOIS CONSUMER FRAUD ACT

(On behalf of Plaintiffs and the Nationwide Class)

68. Plaintiff repeats and incorporates the allegations contained in paragraphs 1 through 47 as if fully set forth herein.

69. Allscripts, operating through its Illinois headquarters, engaged in deceptive, unfair, and unlawful trade acts or practices in the conduct of trade or commerce, in violation of 815 Ill. Comp. Stat. § 505/2, including but not limited to the following:

a. Fraudulently advertising material facts pertaining to its system and data services by representing and advertising that it would maintain security practices and procedures to safeguard its systems and data from cyberattack, including ransomware attacks, which can cause an interruption in the flow of an enterprise's routine and everyday provision of services to its clients and to prevent infiltration of the security system so as to safeguard PHI from unauthorized access;

b. Misrepresenting material facts pertaining to its system and data services by representing and advertising that it would maintain security practices and procedures to safeguard its systems and data from cyberattack, including

ransomware attacks, which can cause an interruption in the flow of an enterprise's routine and everyday provision of services to its clients and to prevent infiltration of the security system so as to safeguard PHI from unauthorized access;

c. Omitting, suppressing, and concealing the material fact of the inadequacy of the security practices and procedures;

d. Engaging in deceptive, unfair, and unlawful trade acts or practices by failing to maintain security practices and procedures to safeguard its systems and data from cyberattack, including ransomware attacks, which can cause an interruption in the flow of an enterprise's routine and everyday provision of services to its clients and to prevent infiltration of the security system so as to safeguard PHI from unauthorized access; and

e. Engaging in deceptive, unfair, and unlawful trade acts or practices by failing to take proper action following the ransomware attack to enact reasonable security practices to safeguard its systems and data from cyberattack, including ransomware attacks, which can cause an interruption in the flow of an enterprise's routine and everyday provision of services to its clients

70. As a direct and proximate result of Allscripts' deceptive trade practices, Plaintiffs and the Class suffered injuries, including but not limited to, complete interruption and disruption of its business of providing services to patients OR complete denial of service and the corresponding inability to operate their business of providing services to patients.

71. The above unfair and deceptive practices and acts by Allscripts were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury that Plaintiffs and

the Class could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

72. Allscripts knew or should have known that its computer systems and security practices and procedures were inadequate and that risk of a ransomware attack, data breach, or theft was high. Allscripts' actions in engaging in the above-named unfair practices and deceptive acts were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of Plaintiffs and the Class.

73. Plaintiff and the Class seek relief under 815 Ill. Comp. Stat. § 505/10a, including, but not limited to, damages, restitution, punitive damages, injunctive relief, and/or attorneys' fees and costs.

COUNT V – VIOLATION OF ILLINOIS UNIFORM DECEPTIVE TRADE PRACTICES ACT

(On behalf of Plaintiffs and the Nationwide Class)

74. Plaintiff repeats and incorporates the allegations contained in paragraphs 1 through 47 as if fully set forth herein.

75. Allscripts, operating through its Illinois headquarters, engaged in deceptive, unfair, and unlawful trade acts or practices in the conduct of trade or commerce, in violation of 815 Ill. Comp. Stat. §§ 510/2(a)(5), and (7).

76. While in the course of its businesses, Allscripts, operating in Illinois, engaged in deceptive trade practices by:

a. Fraudulently advertising material facts pertaining to its system and data services by representing and advertising that it would maintain security practices and procedures to safeguard its systems and data from cyberattack, including ransomware attacks, which can cause an interruption in the flow of

an enterprise's routine and everyday provision of services to its clients and to prevent infiltration of the security system so as to safeguard PHI from unauthorized access;

b. Misrepresenting material facts pertaining to its system and data services by representing and advertising that it would maintain security practices and procedures to safeguard its systems and data from cyberattack, including ransomware attacks, which can cause an interruption in the flow of an enterprise's routine and everyday provision of services to its clients and to prevent infiltration of the security system so as to safeguard PHI from unauthorized access;

77. Allscripts knew or should have known that its computer systems and data security practices were inadequate to safeguard its systems and data from cyberattack, including ransomware attacks, which can cause an interruption in the flow of an enterprise's routine and everyday provision of services to its clients and to prevent infiltration of the security system so as to safeguard PHI from unauthorized access, and engaged in negligent, knowing, and/or willful acts of deception as to those practices and security measures.

78. As a direct and proximate result of Allscripts deceptive and unfair actions, Plaintiff and the Class have been damaged as follows: complete interruption and disruption of its business of providing services to patients OR complete denial of service and the corresponding inability to operate their business of providing services to patients.

REQUEST FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of all Class members proposed in this Complaint, respectfully requests that the Court enter judgment in their favor and against Allscripts as follows:

a. For an Order certifying the Nationwide Class as defined herein, and appointing Plaintiff and her Counsel to represent the Nationwide Class;

b. For equitable relief compelling Allscripts to utilize appropriate methods and policies with respect to ransomware protection.

c. For equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Allscripts' wrongful conduct;

d. For an award of actual damages and compensatory damages, in an amount to be determined;

e. For an award of costs of suit and attorneys' fees, as allowable by law; and

f. 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: January 25, 2018

Respectfully submitted,

/s/ Steven W. Teppler
STEVEN TEPPLER
Illinois Bar Number 6301438
steppler@abbottlawpa.com
BRITTANY FORD*
Florida Bar No. 0117718
ABBOTT LAW GROUP, P.A.
2929 Plummer Cove Road
Jacksonville, FL 32223
Telephone: (904) 292-1111

Facsimile: (904) 292-1220

JOHN A. YANCHUNIS
Florida Bar No. 324681
jyanchunis@ForThePeople.com
MARISA GLASSMAN*
Florida Bar No. 111991
mglassman@ForThePeople.com
PATRICK A. BARTHLE II*
Florida Bar No. 99286
pbarthle@ ForThePeople.com
MORGAN & MORGAN
COMPLEX LITIGATION GROUP
201 N. Franklin Street, 7th Floor
Tampa, Florida 33602
Telephone: (813) 223-5505
Facsimile: (813) 223-5402

JOEL R. RHINE*
North Carolina Bar Number 16028
jrr@rhinelawfirm.com
RHINE LAW FIRM, PC
1612 Military Cutoff Road, Suite 300
Wilmington, NC 28403
Telephone: (910) 772-9960
Facsimile: (910) 772-9062

ROBERT A. CLIFFORD
rac@cliffordlaw.com
SHANNON M. MCNULTY
smm@cliffordlaw.com
CLIFFORD LAW OFFICES
120 N. LaSalle Street, Suite 3100
Chicago, IL 60602
Telephone: (312) 899-9090

Attorneys for Plaintiff and Putative Classes

*motion for admission *pro hac vice* to be submitted