IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS,
EASTERN DIVISION

THE ESTATE OF ANTOINETTE SCARDINA, BY AND THROUGH EXECUTOR RICHARD SCARDINA, INDIVIDUALLY AND ON BEHALF OF ALL OTHERS SIMILARLY SITUATED, Plaintiff, v. ADVOCATE AURORA HEALTH, INC. and ADVOCATE HEALTH AND HOSPITALS CORPORATION d/b/a ADVOCATE CHRIST MEDICAL CENTER, Defendants.	)	**No.** **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Plaintiff, the Estate of Antoinette Scardina, by and through executor Richard Scardina, individually and on behalf of all others similarly situated, through the undersigned counsel, hereby allege the following against Defendants Advocate Christ Medical Center and its owner Advocate Aurora Health Inc. ("Advocate Aurora"), collectively "Defendants." Based upon personal knowledge, information, belief, and investigation of counsel, Plaintiff specifically alleges as follows:

I. INTRODUCTION

1. Plaintiff brings this class action against Defendants for their failure to exercise reasonable care in securing and safeguarding individuals' sensitive personal data. Throughout 2020 and 2021, Defendant Advocate Aurora, owner of Advocate Christ Medical Center, had a series of four data breaches ("Security Breach"). Types of personal data exposed likely included name, date of birth, address, social security number, medical records, lab results, diagnoses,

medications, health insurance information, and dates of service (collectively "Private Information"). Previously, in 2016, a related entity, Advocate Health, paid one of the largest settlements of the year following a data breach that affected over 4 million patients.

2. Defendants' history of data breaches means Defendants should have known how to prevent a data breach and/or mitigate harm from a data breach. Defendants had a heightened duty to protect Plaintiff and Class member data.

3. Between February-March 2021, Richard Scardina, son and executor of the estate of Antoinette Scardina, received a letter from Advocate Christ Medical Center and Advocate Aurora Health describing the data breach of his mother's information.

4. Defendants' security failures enabled the hackers to steal the Private Information of Plaintiff and members of the Class (defined below). These failures put Plaintiff's and Class members' Private Information and interests at serious, immediate, and ongoing risk and, additionally, caused costs and expenses to Plaintiff and Class members associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, emotional grief associated with constant mitigation of personal banking and credit accounts, mitigate and deal with the actual and future consequences of the Security Breach, including, as appropriate, reviewing records for fraudulent charges and healthcare services billed for but not received, reissuing payment cards, purchasing credit monitoring and identity theft protection services, imposition of withdrawal and purchase limits on compromised accounts, initiating and monitoring credit freezes, and the stress, nuisance and annoyance of dealing with all issues resulting from the Security Breach.

5. The Security Breach was caused and enabled by Defendants' violation of their obligations to abide by best practices and industry standards concerning the security of patients

records and Private Information. Defendants failed to comply with security standards and allowed their customers' Private Information to be compromised by cutting corners on security measures that could have prevented or mitigated the Security Breach that occurred.

6. Accordingly, Plaintiff asserts claims for violations of negligence, breach of implied contract, unjust enrichment/quasi-contract, violation of Illinois's Personal Information Protection Act, 815 Ill. Comp. Stat. §§ 530/10(A), et seq., Illinois Consumer Fraud Act, 815 Ill. Comp. Stat. §§ 505, *et seq.*, Illinois Uniform Deceptive Trade Practices Act, Ill. Comp. Stat. §§ 510/2, *et seq.*, and seeks injunctive relief, monetary damages, statutory damages, and all other relief as authorized in equity or by law.

II. JURISDICTION

7. The Court has jurisdiction over Plaintiff's claims under 28 U.S.C. § 1332(d)(2) ("CAFA"), because (a) there are 100 or more Class members, (b) at least one Class member is a citizen of a state that is diverse from Defendants' citizenship, and (c) the matter in controversy exceeds $5,000,000, exclusive of interest and costs.

8. The Court has personal jurisdiction over Defendants because Advocate Christ Medical Center's principal place of business is located here, and Defendants conduct substantial business in this District.

9. Venue is proper in this District under 28 U.S.C. § 1391(b)(1) because Defendants maintain places of business in this District and therefore reside in this District pursuant to 28 U.S.C. § 1391(c)(2). A substantial part of the events or omissions giving rise to the Class's claims also occurred in this District.

III. PARTIES

Plaintiff, the Estate of Antoinette Scardina

10. Plaintiff Antoinette Scardina is represented by her son, Richard Scardina. Richard is the executor of Antoinette Scardina's estate. Richard Scardina is a resident of Illinois. Richard Scardina shared financial accounts with his mother, Antoinette Scardina. Antoinette entered the Advocate Christ Medical Center for COVID-19 on December 6, 2020. Antoinette was a patient for six weeks before she passed away in January 2021. Prior to her passing, Antoinette had only attended Advocate Christ Medical Center for healthcare purposes. Antoinette shared her Private Information with Advocate Christ Medical Center and no other neighboring hospital systems.

11. Between February 2021-March 2021 while Richard Scardina was still grieving his mother's death, he received a data breach notification alerting him that his mother's information was exposed due to Defendants' insecure data systems. Richard Scardina did not find enough of a worthwhile remedy in the letter to keep the letter.

12. After Antoinette's passing, but before Richard received the notification letter, hackers accessed Antoinette's information from Defendants' systems. A series of suspicious behavior occurred throughout Antoinette's accounts, impacting Richard Scardina and his sister.

13. Richard's personal bank account closed a card and sent him a new one.

14. Antoinette's bank account was hacked for the first time in 34 years. $1,000 was removed from the bank account. Antoinette's daughter received a fraudulent call from the bank. While she shared no information, she called the real bank to confirm Antoinette's shared account was protected. Only after calling the real bank did the Scardinas find out hackers stole $1,000 from the account. The family immediately notified the bank, but the bank took 3 weeks to resolve the fraudulent charge with significant time and effort from the Scardinas. Fearing other fraudulent charges, the Scardinas promptly closed the bank account due to the bank hack. Doing so adversely

affected auto-payments for a mortgage and also caused late fees on two credit cards and another bank account. None of these charges were forgiven and the family had to pay out of pocket.

15. Antoinette's daughter received a false charge to a Kohl's store between $300-$500. Luckily, she caught the charge in time to mitigate her harm.

16. Richard had false charges on his Amazon account following the breach and also received suspicious phone calls, texts, emails. He has mitigated his harm by obtaining a T-mobile scam detector for $4 per month.

17. Since the Security Breach, Richard also receives medically-related targeted advertising that he did not previously.

18. Richard has spent an estimated 20-25 hours resolving issues relating to the exposure of his mother's information, their shared account information, and the resulting damage from the Security Breach of their accounts and information.

19. To mitigate his harm, Richard has frozen all of his credit accounts.

20. Exposure of Antoinette's Private Information has forced Richard to extend his grieving process through the stress, nuisance, fear, and annoyance of safeguarding his and Antoinette's personal information and fearing further harm.

Defendants

21. Defendant Advocate Aurora Health is a foreign non-stock corporation incorporated in Delaware, with its principal place of business 750 W Virginia St, Milwaukee, WI 53204. It touts that it "serves nearly 3 million patients annually in Illinois and Wisconsin across more than 500 sites of care."[1]

[1] https://www.linkedin.com/company/aurora-health-care/

22. Defendant Advocate Health and Hospitals Corporation d/b/a/ Advocate Christ Medical Center is a not-for-profit corporation operating in Oak Lawn, Illinois. The registered agent is located at 3075 Highland Parkway 600, Downers Grove, IL 60515. Advocate Christ Medical Center provides emergency care and is a major referral hospital in the Midwest.

23. Defendant Advocate Christ Medical Center is a part of Defendant Advocate Aurora Health Care.

IV. FACTS

24. Defendants provide healthcare services to thousands of patients per year. As part of their business, Defendants stores a vast amount of their patients' Private Information. In doing so, Defendants were entrusted with, and obligated to safeguard and protect, the Private Information of Plaintiff and the Class in accordance with all applicable laws.

25. Advocate Aurora Health experienced a series of data breaches, reported to the Department of Health and Human Services in April 2020, August 2020, September 2020, and July 2021. Collectively, these breaches exposed the Private Information of at least 100,730 records associated with individuals. Any other data breaches that may have occurred have not been publicly reported.

26. Defendants first learned of unusual systems activity whereby an unauthorized party may have gained access to the records that contained patientss Private Information including name, dates of birth, and social security number.

27. Defendants have yet to affirmatively notify impacted patients individually regarding which specific data of theirs were stolen.

28. The Security Breach occurred because Defendants failed to take reasonable measures to protect the Private Information they collected and stored. Among other things,

Defendants failed to implement data security measures designed to prevent this attack, despite repeated public warnings to the healthcare industry about the risk of cyberattacks and the highly publicized occurrence of many similar attacks in the recent past on other healthcare providers. For example, Defendants failed to maintain basic security measures. Defendants failed to disclose to Plaintiff and Class members the material fact that it did not have adequate data security practices to safeguard customers' personal data, and in fact falsely represented that their security measures were sufficient to protect the Personal Information in their possession.

29. Defendants' failure to provide immediate formal notice of the Breach to Plaintiff and Class members exacerbated the injuries resulting from the Breach.

Defendants Failed to Maintain Reasonable and Adequate Security Measures to Safeguard Patients' Private Information Despite Previous Data Breaches

30. Defendants were aware of the risk of data breaches. In 2020, Advocate Aurora employees had their social security numbers and bank account information compromised in an email phishing attack.[2] In April 2020, Advocate Aurora had their network server breached, which they left to be breached again in July 2021. In 2016, Advocate Health paid one of the largest settlements of the year for its data breach affecting over 4 million patients.[3]

31. Defendants are a major regional healthcare system, yet Defendants did not allocate adequate resources for cybersecurity protection of patient information.

32. Under the Health Insurance Portability Act of 1996 ("HIPPA") Defendants had a heightened duty to protect patient Private Information.

[2] https://biztimes.com/advocate-auroras-hr-system-breached-in-email-phishing-campaign/

[3] https://www.cnbc.com/2016/08/04/huge-data-breach-at-health-system-leads-to-biggest-ever-settlement.html

33. Defendants advertise in their Notice of Privacy Practices that they comply with federal privacy law, even while they had already exposed patient information to hackers in violation of HIPPA on four separate occasions.

34. Defendants failed to ensure that proper data security safeguards were being implemented throughout the breach period.

35. Defendants failed to ensure their healthcare operations would not be impacted in case of a data breach.

36. Defendants had obligations created by HIPAA, 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.

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

38. Prior to and during the Security Breach, Defendants promised patients that their Private Information would be kept confidential unless for the reasons listed in their Notice of Privacy Practices or Plaintiff so authorized. Hackers taking Plaintiff' information was not included.

39. Defendants' failure to provide adequate security measures to safeguard patients' Private Information is especially egregious because Defendants operate in a field which has recently been a frequent target of scammers attempting to fraudulently gain access to patients' highly confidential Private Information.

40. Ponemon Institute, an expert in the annual state of cybersecurity, had indicated that in 2020, healthcare institutions were the top target for cyber-attacks.

41. In fact, Defendants have been on notice for years that the medical industry is a prime target for scammers because of the amount of confidential patient information maintained. In 2019 alone, numerous entities in the healthcare sector suffered high-profile data breaches, including Quest Diagnostics and LabCorp.

42. Defendants had resources for years to address their data security. Between 2019-2020, Advocate Aurora's total assets grew from $18,933,369 to $21,449,643.[4] After the first data breach in 2020, Defendants also had the means to take stronger data security steps prior to the following breaches.

Defendants' Data Security Failures and HIPAA Violations

43. Defendants' data security lapses demonstrate that failed to honor their duties and promised by not:

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

b. Adequately protecting patients' Private Information;

c. Properly monitoring their own data security systems for existing intrusions;

d. Ensuring that they employed reasonable data security procedures;

[4] https://www.advocateauroraheath.org/pdfs/aah-2020-audit-report-with-supplemental.pdf

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

h. Implementing 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. Protecting 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. Protecting 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. Ensuring compliance with HIPAA security standard rules by their workforces in violation of 45 C.F.R. § 164.306(a)(4); and/or

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

Damages to Plaintiff and the Class

44. Plaintiff and the Class have been damaged by the compromise of their Private Information in the Security Breach.

45. Plaintiff and the Class have experienced or currently face a substantial risk of out-of-pocket fraud losses such as, *e.g.*, loss of funds from bank accounts, fraudulent charges on credit cards, targeted advertising, suspicious phones calls, and similar identity theft.

46. Class members have or may also incur out of pocket costs for protective measures such as credit freezing or payment for phone scam detection,

47. Plaintiff and Class members suffered a "loss of value" of their Private Information when it was acquired by cyber thieves in the Security Breach. Numerous courts have recognized the propriety of "loss of value" damages in data breach cases.

48. Class members who paid Defendants for their services were also damaged via "benefit of the bargain" damages. Such members of the Class overpaid for a service that was intended to be accompanied by adequate data security but was not. Part of the price Class members paid to Defendants was intended to be used by Defendants to fund adequate data security. Defendants did not properly comply with their data security obligations. Thus, the Class members did not get what they paid for.

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

50. According to the U.S. Department of Justice Bureau of Justice Statistics, an estimated 17.6 million people were victims of one or more incidents of identity theft in 2014.

Among identity theft victims, existing bank or credit accounts were the most common types of misused information.[5]

51. Similarly, the FTC cautions that identity theft wreaks havoc on consumers' finances, credit history, and reputation and can take time, money, and patience to resolve. Identity thieves use stolen personal information for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.[6]

52. Identity thieves can use the victim's Private Information to commit any number of frauds, such as obtaining a job, procuring housing, or even giving false information to police during an arrest. In the medical context, Private Information can be used to submit false insurance claims, obtain prescription drugs or medical devices for black-market resale, or get medical treatment in the victim's name. As a result, Plaintiff and Class members now face a real and continuing immediate risk of identity theft and other problems associated with the disclosure of their Social Security numbers, and will need to monitor their credit and tax filings for an indefinite duration.

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

---

[5] *See* DOJ, *Victims of Identity Theft, 2014* at 1 (Nov. 13, 2017), available at https://bjs.ojp.gov/content/pub/pdf/vit14.pdf

[6] The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 16 C.F.R. § 603.2. The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, social security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number[.]" *Id*.

The Value of Privacy Protections and Private Information

54. The fact that Plaintiff' and Class members' Private Information was stolen—and might presently be offered for sale to cyber criminals—demonstrates the monetary value of the Private Information.

55. At an FTC public workshop in 2001, then-Commissioner Orson Swindle described the value of a consumer's personal information:

> The use of third party information from public records, information aggregators and even competitors for marketing has become a major facilitator of our retail economy. Even [Federal Reserve] Chairman [Alan] Greenspan suggested here some time ago that it's something on the order of the life blood, the free flow of information.[7]

56. Commissioner Swindle's 2001 remarks are even more relevant today, as consumers' personal data functions as a "new form of currency" that supports a $26 billion per year online advertising industry in the United States.[8]

57. The FTC has also recognized that consumer data is a new (and valuable) form of currency. In an FTC roundtable presentation, another former Commissioner, Pamela Jones Harbour, underscored this point:

> Most consumers cannot begin to comprehend the types and amount of information collected by businesses, or why their information

[7] Tr. at 8:2-8, Federal Trade Commission, *Public Workshop: The Information Marketplace: Merging and Exchanging Consumer Data* (Mar. 13, 2001) available at https://www.ftc.gov/sites/default/files/documents/public_events/information-marketplace-merging-and-exchanging-consumer-data/transcript.pdf

[8] *See* Julia Angwin & Emily Steel, *Web's Hot New Commodity: Privacy*, The Wall Street Journal (Feb. 28, 2011), https://www.wsj.com/articles/SB10001424052748703529004576160764037920274

> may be commercially valuable. Data is currency. The larger the data set, the greater potential for analysis—and profit.[9]

58. Recognizing the high value that consumers place on their Private Information, many companies now offer consumers an opportunity to sell this information.[10] The idea is to give consumers more power and control over the type of information that they share and who ultimately receives that information. And, by making the transaction transparent, consumers will make a profit from their Private Information. This business has created a new market for the sale and purchase of this valuable data.

59. Consumers place a high value not only on their Private Information, but also on the privacy of that data. Researchers have begun to shed light on how much consumers value their data privacy, and the amount is considerable. Indeed, studies confirm that the average direct financial loss for victims of identity theft in 2014 was $1,349.[11]

60. At all relevant times, Defendants were well-aware, or reasonably should have been aware, that the Private Information it maintains is highly sensitive and could be used for wrongful purposes by third parties, such as identity theft and fraud. Defendants should have particularly been aware of these risks given the significant number of data breaches affecting the medical industry.

61. Had Defendants remedied the deficiencies in their security systems after their first Security Breach, followed industry guidelines, and adopted security measures recommended by

---

[9] *Statement of FTC Commissioner Pamela Jones Harbour—Remarks Before FTC Exploring Privacy Roundtable*, (Dec. 7, 2009), https://www.ftc.gov/sites/default/files/documents/public_statements/remarks-ftc-exploring-privacy-roundtable/091207privacyroundtable.pdf

[10] *Web's Hot New Commodity: Privacy*, *supra* note 7.

[11] *See* DOJ, *Victims of Identity Theft, 2014*, *supra* note 3, at 6.

experts in the field, Defendants would have prevented intrusion into their systems and, ultimately, the theft of their patients' Private Information.

62. Given these facts, any company that transacts business with patients and then compromises the privacy of patients' Private Information has thus deprived patients of the full monetary value of their transaction with the company.

63. Due to damage from Defendants, Plaintiff and the other Class members now face a greater risk of continuous identity theft.

V. CLASS ACTION ALLEGATIONS

64. Plaintiff brings all counts, as set forth below, individually and as a class action, pursuant to the provisions of Rule 23 of the Federal Rules of Civil Procedure, on behalf of a Nationwide Class defined as:

> All persons who had their Private Information submitted to Defendants or Defendants' affiliates and/or whose Private Information was compromised as a result of the data breach(es) discovered between 2020 through 2021, (the "Nationwide Class").

65. In addition to and/or in the alternative to claims asserted on behalf of the Nationwide Class, Plaintiff asserts claims on behalf of the following Illinois subclass ("Subclass"):

> All residents of Illinois who had their Private Information submitted to Defendants or Defendants' affiliates and/or whose Private Information was compromised as a result of the data breach(es) discovered between 2020 through 2021.

66. Excluded from both the Nationwide Class and the Subclass are Defendants and Defendants' affiliates, parents, subsidiaries, employees, officers, agents, and directors. Also excluded is any judicial officer presiding over this matter and the members of their immediate families and judicial staff.

67. Certification of Plaintiff's claims for class-wide treatment is appropriate because Plaintiff can prove the elements of her claims on a class-wide basis using the same evidence as would be used to prove those elements in individual actions alleging the same claims.

68. **Numerosity—Federal Rule of Civil Procedure 23(a)(1).** The members of the Class are so numerous that joinder of all Class members would be impracticable. On information and belief, the Nationwide Class and Subclass both number in the tens of thousands.

69. **Commonality and Predominance—Federal Rule of Civil Procedure 23(a)(2) and 23(b)(3).** Common questions of law and fact exist as to all members of the Class and predominate over questions affecting only individual members of the Class. Such common questions of law or fact include, *inter alia*:

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

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

c. Whether Defendants properly implemented their purported security measures to protect Plaintiff's and the Class's Private Information from unauthorized capture, dissemination, and misuse;

d. Whether Defendants took reasonable measures to determine the extent of the Security Breach after they first learned of same;

e. Whether Defendants disclosed Plaintiff' and the Class's Private Information in violation of the understanding that the Private Information was being disclosed in confidence and should be maintained;

f. Whether Defendants' conduct constitutes breach of an implied contract;

g. Whether Defendants willfully, recklessly, or negligently failed to maintain and execute reasonable procedures designed to prevent unauthorized access to Plaintiff' and the Class's Private Information;

h. Whether Defendants were negligent in failing to properly secure and protect Plaintiff' and the Class's Private Information;

i. Whether Defendants was unjustly enriched by their actions; and

j. Whether Plaintiff and the other members of the Class are entitled to damages, injunctive relief, or other equitable relief, and the measure of such damages and relief.

70. Defendants engaged in a common course of conduct giving rise to the legal rights sought to be enforced by Plaintiff, on behalf of herself and other members of the Class. Similar or identical common law violations, business practices, and injuries are involved. Individual questions, if any, pale by comparison, in both quality and quantity, to the numerous common questions that predominate in this action.

71. **Typicality—Federal Rule of Civil Procedure 23(a)(3).** Plaintiff's claims are typical of the claims of the other members of the Class because, among other things, all Class members were similarly injured through Defendants' uniform misconduct described above and were thus all subject to the Security Breach alleged herein. Further, there are no defenses available to Defendants that are unique to Plaintiff.

72. **Adequacy of Representation—Federal Rule of Civil Procedure 23(a)(4).** Plaintiff is an adequate representative of the Nationwide Class and the Subclass because their interests do not conflict with the interests of the Classes they seek to represent, they have retained

counsel competent and experienced in complex class action litigation, and Plaintiff will prosecute this action vigorously. The Class's interests will be fairly and adequately protected by Plaintiff and their counsel.

73. **Injunctive Relief-Federal Rule of Civil Procedure 23(b)(2).** Defendants have acted and/or refused to act on grounds that apply generally to the Class, making injunctive and/or declaratory relief appropriate with respect to the Class under Fed. Civ. P. 23 (b)(2).

74. **Superiority—Federal Rule of Civil Procedure 23(b)(3).** A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. The damages or other financial detriment suffered by Plaintiff and the other members of the Class are relatively small compared to the burden and expense that would be required to individually litigate their claims against Defendants, so it would be impracticable for members of the Class to individually seek redress for Defendants' wrongful conduct. Even if members of the Class could afford individual litigation, the court system could not. Individualized litigation creates a potential for inconsistent or contradictory judgments and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of a single adjudication, economy of scale, and comprehensive supervision by a single court.

VI. CAUSES OF ACTION

COUNT I
Negligence

75. Plaintiff fully incorporates by reference all of the above paragraphs, as though fully set forth herein.

76. Upon Defendants' accepting and storing the Private Information of Plaintiff and the Class in their computer systems and on their networks, Defendants undertook and owed a duty to Plaintiff and the Class to exercise reasonable care to secure and safeguard that information and to use commercially reasonable methods to do so. Defendants knew that the Private Information was private and confidential and should be protected as private and confidential.

77. Defendants owed a duty of care not to subject Plaintiff' and the Class's Private Information to an unreasonable risk of exposure and theft because Plaintiff and the Class were foreseeable and probable victims of any inadequate security practices.

78. Defendants owed numerous duties to Plaintiff and the Class, including the following:

a. to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting and protecting Private Information in their possession;

b. to protect Private Information using reasonable and adequate security procedures and systems that are compliant with industry-standard practices; and

c. to implement processes to quickly detect a data breach and to timely act on warnings about data breaches.

79. Defendants also breached their duty to Plaintiff and the Class members to adequately protect and safeguard Private Information by disregarding standard information security principles, despite obvious risks, and by allowing unmonitored and unrestricted access to unsecured Private Information. Furthering their dilatory practices, Defendants failed to provide adequate supervision and oversight of the Private Information with which they were and are entrusted, in spite of the known risk and foreseeable likelihood of breach and misuse, which

permitted a malicious third party to gather Plaintiff's and Class members' Private Information and potentially misuse the Private Information and intentionally disclose it to others without consent.

80. Defendants knew, or should have known, of the risks inherent in collecting and storing Private Information and the importance of adequate security. Defendants knew or should have known about numerous well-publicized data breaches within the medical industry.

81. Defendants knew, or should have known, that their data systems and networks did not adequately safeguard Plaintiff' and Class members' Private Information.

82. Defendants breached their duties to Plaintiff and the Class members by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and Class members' Private Information.

83. Because Defendants knew that a breach of their systems would damage thousands of their customers, including Plaintiff and the Class members, Defendants had a duty to adequately protect their data systems and the Private Information contained thereon.

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

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

the medical information at issue in this case constitutes "protected health information" within the meaning of HIPAA.

86. Additionally, HIPPA requires that only authorized parties may access Private Information of an individual who has been deceased for less than 50 years. 45 C.F.R. 160.103, paragraph (2)(iv).

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

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

89. Defendants' own conduct also created a foreseeable risk of harm to Plaintiff and Class members and their Private Information. Defendants' misconduct included failing to: (1) secure Plaintiff's and the Class members' Private Information; (2) comply with industry standard security practices; (3) implement adequate system and event monitoring; and (4) implement the systems, policies, and procedures necessary to prevent this type of data breach.

90. Defendants breached their duties, and thus was negligent, by failing to use reasonable measures to protect Class members' Private Information, and by failing to provide timely notice of the Security Breach. The specific negligent acts and omissions committed by Defendants 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 Defendants' networks and systems;

c. Allowing unauthorized access to Class members' Private Information;

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

e. Failing to timely notify Class members about the Security Breach so that they could take appropriate steps to mitigate the potential for identity theft and other damages

91. Through Defendants' acts and omissions described in this Complaint, including their failure to provide adequate security and their failure to protect Plaintiff's and Class members' Private Information from being foreseeably captured, accessed, disseminated, stolen and misused, Defendants unlawfully breached their duty to use reasonable care to adequately protect and secure Plaintiff' and Class members' Private Information during the time it was within Defendants' possession or control.

92. Defendants' conduct was grossly negligent and departed from all reasonable standards of care, including, but not limited to: failing to adequately protect the Private Information and failing to provide Plaintiff and Class members with timely notice that their sensitive Private Information had been compromised.

93. Neither Plaintiff nor the other Class members contributed to the Security Breach and subsequent misuse of their Private Information as described in this Complaint.

94. As a direct and proximate cause of Defendants' conduct, Plaintiff and Class members suffered damages as alleged above.

95. Plaintiff and Class members are also entitled to injunctive relief requiring Defendants to, *e.g.*, (i) strengthen their data security systems and monitoring procedures; (ii)

submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide lifetime free credit monitoring to all Class members.

COUNT II
Breach of Implied Contract

96. Plaintiff fully incorporates by reference all of the above paragraphs, as though fully set forth herein.

97. Defendants solicited and invited Class members to provide their Private Information as part of Defendants' regular business practices. When Plaintiff and Class members made and paid for purchases of Defendants' services and products, they provided their Private Information to Defendants.

98. In so doing, Plaintiff and Class members entered into implied contracts with Defendants pursuant to which Defendants agreed to safeguard and protect such information and to timely detect any breaches of their Private Information. In entering into such implied contracts, Plaintiff and Class members reasonably believed and expected that Defendants' data security practices complied with relevant laws and regulations, including HIPAA, and were consistent with industry standards.

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

100. Plaintiff and Class members would not have provided and entrusted their Private Information with Defendants in the absence of the implied contract between them and Defendants.

101. Plaintiff and Class members fully performed their obligations under the implied contracts with Defendants.

102. Defendants breached the implied contracts they made with Plaintiff and Class members by failing to safeguard and protect their Private Information and by failing to timely detect the data breach within a reasonable time.

103. As a direct and proximate result of Defendants' breaches of the implied contracts between Defendants, Plaintiff and Class members, Plaintiff and Class members sustained actual losses and damages as described in detail above.

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

COUNT III
Unjust Enrichment/Quasi-Contract

105. Plaintiff fully incorporates by reference all of the above paragraphs, as though fully set forth herein.

106. Plaintiff and Class members conferred a monetary benefit on Defendants. Specifically, they purchased goods and services from Defendants and provided Defendants with their Private Information. In exchange, Plaintiff and Class members should have received from Defendants the goods and services that were the subject of the transaction and should have been entitled to have Defendants protect their Private Information with adequate data security.

107. Defendants knew that Plaintiff and Class members conferred a benefit on them and accepted and has accepted or retained that benefit. Defendants profited from Plaintiff's purchases and used Plaintiff's and the Class members' Private Information for business purposes.

108. Defendants failed to secure Plaintiff's and the Class members' Private Information and, therefore, did not provide full compensation for the benefit of the Plaintiff's and Class members' Private Information provided.

109. Defendants acquired the Private Information through inequitable means as they failed to disclose the inadequate security practices previously alleged.

110. If Plaintiff and the Class members knew that Defendants would not secure their Private Information using adequate security, they would not have made purchases at Defendants' stores.

111. Plaintiff and Class members have no adequate remedy at law.

112. Under the circumstances, it would be unjust for Defendants to be permitted to retain any of the benefits that Plaintiff and Class members conferred on them.

113. Defendants should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and Class members, proceeds that they unjustly received from them. In the alternative, Defendants should be compelled to refund the amounts that Plaintiff and Class members overpaid.

COUNT IV
ILLINOIS PERSONAL INFORMATION PROTECTION ACT, 815 ILL. COMP. STAT. §§ 530/10(A), ET SEQ.

114. Plaintiff fully incorporates by reference all of the above paragraphs, as though fully set forth herein.

115. As corporations that handle, collect, disseminate, and otherwise deal with Private, personal information, Defendants are Data Collectors, as defined in 815 Ill. Comp. Stat. § 530/5.

116. Plaintiff's and the Class members' Private Information includes personal information as covered under 815 Ill. Comp. State. § 530/5.

117. As a Data Collector, Defendants are required to notify Plaintiff and the Class members of a breach of their data security system in the most expedient time possible and without unreasonable delay pursuant to 815 Ill. Comp. Stat. § 530/10(a).

118. By failing to disclose the data breach in the most expedient time possible and without unreasonable delay, Defendants violated 815 Ill. Comp. Stat. § 530/10(a).

119. Pursuant to 815 Ill. Comp. Stat. § 530/20, a violation of 815 Ill. Comp. Stat. § 530/10(a) constitutes an unlawful practice under the Illinois Consumer Fraud and Deceptive Business Practices Act.

120. As a direct and proximate result of Defendants' violations of 815 Ill. Comp. Stat. § 530/10(a), Plaintiff and Class members suffered damages, as described above.

121. Plaintiff and Illinois Class members seek relief under 815 Ill. Comp. Stat. § 510/3 for the harm they suffered because of Defendants' willful conduct.

COUNT V
ILLINOIS CONSUMER FRAUD ACT, 815 ILL. COMP. STAT. §§ 505, ET SEQ.

122. Plaintiff fully incorporates by reference all of the above paragraphs, as though fully set forth herein.

123. Defendants are "persons" as defined by 815 Ill. Comp. Stat. §§ 505/1(c).

124. Plaintiff and the Class members are "consumers" as defined by 815 Ill. Comp. Stat. §§ 505/1(e).

125. Defendants' conduct as described herein was in the conduct of "trade" or "commerce" as defined by 815 Ill. Comp. Stat. § 505/1(f).

126. Defendants' deceptive, unfair, and unlawful practices, in violation of 815 Ill. Comp. Stat. § 505/2, include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Class members' Private Information, which was a direct and proximate cause of the Security Breach;

b. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Class member's Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, 815 Ill. Comp. Stat. § 505/2RR, and the Illinois Uniform Deceptive Trade Practices Act, 815 Ill. Comp. Stat. § 510/2(a), which was direct and proximate cause of the Security Breach.

c. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff's and Class member's Private Information, including by implementing and maintaining reasonable security measures;

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

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Class member's Private Information;

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

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of

Plaintiff's and Class member's Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, Illinois laws regulating the use and disclosure of Social Security Numbers, 815 Ill. Comp. Stat. § 505/2RR, and the Illinois Uniform Deceptive Trade Practices Act, 815 Ill. Comp. Stat. § 510/2(a).

127. Defendants' representations and omissions were material because they were likely to deceive reasonable consumers and/or patients about the adequacy of Defendants' data security and ability to protect the confidentiality of patients' Private Information.

128. Defendants intended to mislead Plaintiff and Class members and induce them to rely on their misrepresentations and omissions.

129. The above unfair and deceptive practices and acts by Defendants were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury that these consumers could not reasonably avoid; this substantial injury outweighed any benefits to patients, consumers, or to competition.

130. Defendants acted intentionally, knowingly, and maliciously to violate Illinois's Consumer Fraud Act, and recklessly disregarded Plaintiff and Class member's rights.

131. As a direct and proximate result of Defendants' unfair, unlawful, and deceptive acts and practices, Plaintiff and Class members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft, time and expenses related to monitoring financial accounts for fraudulent activity, an increased, imminent risk of fraud and identity theft, loss of value of Private Information, and nuisance, emotional grief, stress, and annoyance.

132. Plaintiff and the Class members seek all monetary and non-monetary relief allowed by law, including damages, restitution, punitive damages, injunctive relief, and reasonable attorneys' fees and costs.

COUNT VI
ILLINOIS UNIFORM DECEPTIVE TRADE PRACTICES ACT, 815 ILL. COMP. STAT. §§ 510/2, *ET SEQ*.

133. Plaintiff fully incorporate by reference all of the above paragraphs, as though fully set forth herein.

134. Defendants are "persons" as defined by 815 Ill. Comp. Stat. §§ 510/1(5).

135. Defendants engaged in deceptive trade practices in the conduct of their business, in violation of 815 Ill. Comp. Stat. §§510/2(a), including:

a. Representing that goods or services have characteristics that they do not have;

b. Representing that goods or services are of a particular standard, quality, or grade if they are of another;

c. Advertising goods or services with intent not to sell them as advertised; and

d. Engaging in other conduct that creates a likelihood of confusion or misunderstanding.

136. Defendants' deceptive trade practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's and Class members' Private Information, which was a direct and proximate cause of the Security Breach;

b. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Class members' Private Information, including duties imposed by the FTC Act U.S.C. § 45, Illinois laws regulating the uses and

disclosure of Private Information, 815 Ill. Comp. Stat § 505/2RR, and the Illinois Uniform Deceptive Trade Practices Act, 815 Ill. Comp. Stat. §510/2(a), which was a direct and proximate cause of the Security breach;

c. Misrepresenting that Plaintiff's and Class member's Private Information would be protected and held confidentially, including by implementing and maintain reasonable security measures;

d. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Class members' Private Information;

e. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff's and Class member's Private Information; and

f. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Class member's Private Information.

137. Defendants' representation and omissions were material because they were likely to deceive reasonable consumers and/or patients about the Security Breach and Defendants' ability to protect the confidentiality of Private Information.

138. The above unfair and deceptive practices and acts by Defendants were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to Plaintiff and Class members that they could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

139. As a direct and proximate result of Defendants' unfair, unlawful, and deceptive trade practices, Plaintiff and Class members have suffered and will continue to suffer injury,

ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft, time and expenses related to monitoring their financial accounts for fraudulent activity, an increased and imminent risk of fraud and identity theft, and loss of value of their Personal Information.

140. Plaintiff and Class members seek all monetary and non-monetary relief allowed by law, including injunctive relief and reasonable attorney's fees.

REQUEST FOR RELIEF

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

A. Declaring that this action is a proper class action, certifying the Nationwide Class as requested herein, designating Plaintiff as Nationwide Class and Subclass Representative, and appointing Class Counsel as requested in Plaintiff' expected motion for class certification;

B. Ordering Defendants to pay actual damages to Plaintiff and the other members of the Class;

C. Ordering Defendants to pay punitive damages, as allowable by law, to Plaintiff and the other members of the Class;

D. Ordering injunctive relief requiring Defendants to, *e.g.*: (i) strengthen their data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide free credit monitoring to all Class members;

E. Ordering Defendants to pay attorneys' fees and litigation costs to Plaintiff and their counsel;

F. Ordering Defendants to pay equitable relief, in the form of disgorgement and restitution, and injunctive relief as may be appropriate;

G. Ordering Defendants to pay both pre- and post-judgment interest on any amounts awarded; and

H. Ordering such other and further relief as may be just and proper.

Date: July 16, 2021

Respectfully submitted,

By: /s/ *Stacy M. Bardo*
stacy@bardolawpc.com
Bardo Law, P.C.
22 West Washington St., Suite 1500
Chicago, Illinois 60602
Tel: (312) 219-6980
Fax: (312) 219-6981

Jason S. Rathod
jrathod@classlawdc.com
Nicholas A. Migliaccio
nmigliaccio@classlawdc.com
Migliaccio & Rathod LLP[12]
412 H Street NE
Washington, DC 20002
Tel: (202) 470-3520
Fax: (202) 800-2730

Counsel for Plaintiff

[12] Will seek *pro hac vice* admission

ClassAction.org