

YES NO

EXHIBITS

CASE NO. 24Ch00869

DATE: 2-9-24

CASE TYPE: Class

PAGE COUNT: 32

CASE NOTE

Hearing Date: 6/12/2024 9:30 AM
Location: Court Room 2402
Judge: Price Walker, Allen

FILED
2/9/2024 5:20 PM
IRIS Y. MARTINEZ
CIRCUIT CLERK
COOK COUNTY, IL
2024CH00869
Calendar, 3
26355414

FILED DATE: 2/9/2024 5:20 PM 2024CH00869

12-Person Jury

Chancery Division Civil Cover Sheet
General Chancery Section

(12/01/20) CCH 0623

IN THE CIRCUIT COURT OF COOK COUNTY, ILLINOIS COUNTY DEPARTMENT, CHANCERY DIVISION

Byron Foxie, legal guardian and parent of Tige W. Foxie,
individually and on behalf of all other similarly situated

Plaintiff

2024CH00869

Case No: _____

v.

Ann & Robert H. Lurie Children's Hospital of Chicago

Defendant

CHANCERY DIVISION CIVIL COVER SHEET GENERAL CHANCERY SECTION

A Chancery Division Civil Cover Sheet - General Chancery Section shall be filed with the initial complaint in all actions filed in the General Chancery Section of Chancery Division. The information contained herein is for administrative purposes only. Please check the box in front of the appropriate category which best characterizes your action being filed.

Only one (1) case type may be checked with this cover sheet.

- | | |
|--|---|
| 0005 <input type="checkbox"/> Administrative Review | 0017 <input type="checkbox"/> Mandamus |
| 0001 <input checked="" type="checkbox"/> Class Action | 0018 <input type="checkbox"/> Ne Exeat |
| 0002 <input type="checkbox"/> Declaratory Judgment | 0019 <input type="checkbox"/> Partition |
| 0004 <input type="checkbox"/> Injunction | 0020 <input type="checkbox"/> Quiet Title |
| 0007 <input type="checkbox"/> General Chancery | 0021 <input type="checkbox"/> Quo Warranto |
| 0010 <input type="checkbox"/> Accounting | 0022 <input type="checkbox"/> Redemption Rights |
| 0011 <input type="checkbox"/> Arbitration | 0023 <input type="checkbox"/> Reformation of a Contract |
| 0012 <input type="checkbox"/> Certiorari | 0024 <input type="checkbox"/> Rescission of a Contract |
| 0013 <input type="checkbox"/> Dissolution of Corporation | 0025 <input type="checkbox"/> Specific Performance |
| 0014 <input type="checkbox"/> Dissolution of Partnership | 0026 <input type="checkbox"/> Trust Construction |
| 0015 <input type="checkbox"/> Equitable Lien | 0050 <input type="checkbox"/> Internet Take Down Action (Compromising Images) |
| 0016 <input type="checkbox"/> Interpleader | <input type="checkbox"/> Other (specify) _____ |

Atty. No.: 63014 Pro Se 99500

Atty Name: T. J. Jesky

Atty. for: Law Offices of T. J. Jesky

Address: 205 N. Michigan Ave., Suite 810

City: Chicago State: IL

Zip: 60601

Telephone: 312-894-0130

Primary Email: tj@jeskylaw.com

Pro Se Only: I have read and agree to the terms of the Clerk's Clerk's Office Electronic Notice Policy and choose to opt in to electronic notice from the Clerk's office for this case at this email address:

Email: _____

Iris Y. Martinez, Clerk of the Circuit Court of Cook County, Illinois
cookcountyclerkofcourt.org

**IN THE CIRCUIT COURT OF COOK COUNTY, ILLINOIS
COUNTY DEPARTMENT, CHANCERY DIVISION**

BYRON FOXIE, legal guardian and parent of
TIGE W. FOXIE, individually and on behalf of
all other similarly situated,

Plaintiff,

vs.

ANN & ROBERT H. LURIE CHILDREN'S
HOSPITAL OF CHICAGO.

Defendant.

CASE NO.: 2024CH00869

CLASS ACTION

JURY TRIAL DEMANDED

CLASS ACTION COMPLAINT

Plaintiff, BYRON FOXIE, legal guardian and parent of TIGE W. FOXIE, (collectively "Plaintiff") brings this Class Action Complaint ("Complaint") against Defendant, ANN & ROBERT H. LURIE CHILDREN'S HOSPITAL OF CHICAGO s (hereinafter, "Defendant" or "LURIE") as an individual and on behalf of all others similarly situated, and alleges, upon personal knowledge as to his own actions and his counsels' investigation, and upon information and belief as to all other matters, as follows:

NATURE OF THE ACTION

1. Plaintiff brings this class action against LURIE for its failure to properly secure and safeguard Plaintiff's and Class Members' sensitive information, including their names, dates of birth, addresses, and medical and treatment information, which is protected health information ("PHI" and collectively with PII, "Private Information") as defined by the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") (collectively, "Private Information").

2. On or about January 31, 2024, the Defendant was subject to a cybersecurity attack where the Defendant's network system was compromised involving Private Information files containing information about LURIE's current and former patients.

3. As a children's hospital, the Defendant collects and maintains the sensitive, non-public Private Information of former and current LURIE's patients, including the Plaintiff and Class Members.

4. Defendant retains this Private Information for many years and even after the patient-physician relationship has ended.

5. In maintaining and safe-keeping Private Information of Plaintiff and Class Members, Defendant assumes legal and equitable duties to those individuals to protect and safeguard that information from unauthorized access.

6. Defendant failed to adequately protect Plaintiff's and Class Members' Private Information. This Private Information was compromised due to Defendant's negligent acts and omissions and their failure to protect its affiliates' patients' sensitive data.

7. It appears that this cybersecurity attack allowed unauthorized access to the Plaintiff's and Class Members' Private Information. The present and continuing risk to victims of the cybersecurity attack will remain for their respective lifetimes.

8. As a result of Defendant's inadequate security and breach of their duties a cybersecurity attack took place, and the Plaintiff and Class Members' Private Information was accessed by the cybersecurity attacker.

9. This action seeks to remedy these failings and their consequences. Plaintiff brings this action on behalf of himself and all persons whose Private Information is exposed as a result

of the cybersecurity breach, which started on or about January 31, 2024 and has not been contained as of the date of filing this Class Action Complaint.

10. Plaintiff brings this action on behalf of all persons whose Private Information was compromised, as a result of Defendant' failure to: (i) adequately protect the Private Information of Plaintiff and Class Members; (ii) warn Plaintiff and Class Members of Defendant's inadequate information security practices; and (iii) effectively secure hardware containing protected Private Information using reasonable and effective security procedures free of vulnerabilities and incidents.

11. Defendant's conduct amounts to negligence and violates federal and state statutes.

12. Plaintiff and Class Members have suffered injury as a result of Defendant's negligent conduct. These injuries include: (i) invasion of privacy; (ii) theft of their Private Information; (iii) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the cybersecurity attack; (iv) lost opportunity costs associated with attempting to mitigate the actual consequences of the cybersecurity attack; (v) statutory damages; (vi) nominal damages; and (vii) the continued and certainly increased risk to their Private Information.

13. Plaintiff, on behalf of himself and all other Class Members, asserts claims for negligence, negligence per se, breach of fiduciary duty, breach of implied contract, unjust enrichment, and violations of the Illinois Consumer Fraud and Deceptive Business Practices Act, and seeks declaratory relief, injunctive relief, monetary damages, statutory damages, punitive damages, equitable relief, and all other relief authorized by law.

PARTIES

14. Plaintiff has been a patient of LURIE's, on and off, between 2010 and 2017.

15. Since 2019, the Plaintiff currently has an active and ongoing lawsuit against LURIE's in the Circuit Court of Cook County, Illinois, Law Division based on negligence and

spoliation of evidence in their electronic medical system, among other counts. It was this electronic medical system, that is a target for the cybersecurity attack.

16. Defendant is a not-for-profit Corporation, properly recognized and sanctioned by the laws of the State of Illinois, with its headquarters located at 225 E. Chicago Ave., Chicago, IL 60611, in Cook County.

17. According to LURIE’s website, “more than 239,000 children receive the highest-quality medical care at Lurie Children’s each year,” and “Lurie Children’s treats more children insured by Medicaid than any other hospital in Illinois.”

JURISDICTION AND VENUE

18. This Court has general personal jurisdiction over Defendant, pursuant to 735 ILCS 5/2-209, because the Defendant is organized under the laws of this state and regularly does business or solicits business, engages in other persistent courses of conduct, maintains its electronic medical records-record keeping and/or derives substantial revenue from services provided to individuals in Cook County and in the State of Illinois, and expects or should reasonably expect to be in court here.

19. This Court has subject matter jurisdiction over this matter pursuant to Ill. Const. 1970, art. VI, § 9.

20. Venue is proper in Cook County pursuant to 735 ILCS 5/2-101 because LURIE’s conducts its usual and customary business in this County and because a substantial portion of the events complained of occurred in this County.

BACKGROUND

Overview

21. LURIE's is a nationally ranked pediatric acute care 360-bed children's hospital located in Chicago, Illinois.

22. Plaintiff and Class Members are current and former LURIE patients.

23. As a condition of receiving medical services at LURIE, they require that the Plaintiff and Class Members, entrust Defendant with highly sensitive personal information.

24. Upon information and belief, Defendant made representations to their patients, including Plaintiff and Class Members, that the Private Information collected from them as a condition of obtaining medical services at LURIE's would be kept safe, confidential, that the privacy of that information would be maintained, and that Defendant would delete any sensitive information after it was no longer required to maintain it.

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

26. Defendant has a duty to adopt reasonable measures to protect the Private Information of Plaintiff and Class Members from involuntary disclosure to third parties and to audit, monitor, and verify the integrity of its IT vendors and affiliates. Defendant has a legal duty to keep Private Information safe and confidential.

27. Defendant has obligations created by FTC Act, HIPAA, contract, and representations made to Plaintiff and Class Members, to keep their Private Information confidential and to protect it from unauthorized access and disclosure.

28. Defendant derived a substantial economic benefit from collecting Plaintiff's and Class Members' Private Information. Without the required submission of Private Information, Defendant could not perform the services they provide.

29. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' Private Information, Defendant assumed legal and equitable duties and knew or should have known, that it was responsible for protecting Plaintiff's and Class Members' Private Information from disclosure.

The Cybersecurity Attack

30. On or about January 31, 2024, the Defendant became aware of a cybersecurity attack on the electronic systems.

31. Upon learning of the cybersecurity attack, the Defendant notified the public that to mitigate damages they turned off their internal phone system, internal emails, their electronic health record system and patient portals.

32. By that time, the cybersecurity attack had already taken place and the Defendant's internal systems were compromised.

33. On February 8, 2024, Defendants, confirmed to the public, that its network had been accessed by a "known criminal threat actor."

34. The affected breach of the security systems may have included names, and some combination of the following: dates of birth, addresses, medical record numbers, medical information, and dates/times of service.

35. Defendant did not use reasonable security procedures and practices appropriate to the nature of the sensitive information they were maintaining for Plaintiff and Class Members, causing the exposure of Private Information.

36. By obtaining, collecting, and storing the Private Information of Plaintiff and Class Members, Defendant assumed legal and equitable duties and knew or should have known that they were responsible for protecting the Private Information from disclosure. Moreover, Defendant owed a duty to audit, monitor, and verify the integrity of its own IT system, its vendors and affiliates.

37. Defendant could have prevented this cybersecurity attack by properly securing its files and file servers containing the Private Information of Plaintiff and Class Members or by exercising due diligence in selecting its IT vendors and properly auditing those vendor's security practices.

38. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the Private Information of Plaintiff and Class Members and of the foreseeable consequences that would occur if Defendant's data security systems were breached, including, specifically, the significant costs that would be imposed on Plaintiff and Class Members as a result of a breach.

39. The injuries to Plaintiff and Class Members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for the Private Information of Plaintiff and Class Members.

40. The ramifications of Defendant's failure to keep secure the Private Information of Plaintiff and Class Members are long lasting and severe. Once Private Information is stolen—particularly Social Security numbers and Private Information—fraudulent use of that information and damage to victims may continue for years.

41. The Defendant knew, or should have known, the importance of safeguarding the Private Information entrusted to them by Plaintiff and Class Members and of the foreseeable

consequences if its data security systems, or those on which it transferred Private Information, were breached. This includes the significant costs imposed on Plaintiff and Class Members as a result of a breach.

42. The Defendant failed to take adequate cybersecurity measures to prevent the cybersecurity breach.

Defendant Failure with HIPAA Guidelines

43. The Defendant failed to take adequate cybersecurity measures to prevent the cybersecurity attack.

44. Defendant is covered under HIPAA (45 C.F.R. § 160.102) and is required to comply with the HIPAA Privacy Rule and Security Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and E (“Standards for Privacy of Individually Identifiable Health Information”), and Security Rule (“Security Standards for the Protection of Electronic Protected Health Information”), 45 C.F.R. Part 160 and Part 164, Subparts A and C.

45. Defendant is subject to the rules and regulations for safeguarding electronic medical information pursuant to the Health Information Technology Act (“HITECH”). 28 See 42 U.S.C. §17921, 45 C.F.R. § 160.103.

46. HIPAA’s Privacy Rule or Standards for Privacy of Individually Identifiable Health Information establishes national standards for the protection of health information.

47. HIPAA’s Privacy Rule or Security Standards for the Protection of Electronic Protected Health Information establishes a national set of security standards for protecting health information that is kept or transferred in electronic form.

48. HIPAA requires “compl[iance] with the applicable standards, implementation specifications, and requirements” of HIPAA “with respect to electronic protected health information.” 45 C.F.R. § 164.302.

49. “Electronic protected health information” is “individually identifiable health information ... that is (i) transmitted by electronic media; maintained in electronic media.” 45 C.F.R. § 160.103.

50. HIPAA’s Security Rule requires Defendant to do the following:

- a. Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits;
- b. Protect against any reasonably anticipated threats or hazards to the security or integrity of such information;
- c. Protect against any reasonably anticipated uses or disclosures of such information that are not permitted; and
- d. Ensure compliance by its workforce.

51. HIPAA also requires Defendant to “review and modify the security measures implemented ... as needed to continue provision of reasonable and appropriate protection of electronic protected health information.” 45 C.F.R. § 164.306(e). Additionally, Defendant are required under HIPAA to “[i]mplement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights.” 45 C.F.R. § 164.312(a)(1).

52. HIPAA and HITECH also obligate Defendant to implement policies and procedures to prevent, detect, contain, and correct security violations, and to protect against uses or disclosures of electronic protected health information that are reasonably anticipated but not

permitted by the privacy rules. See 45 C.F.R. § 164.306(a)(1) and § 164.306(a)(3); see also 42 U.S.C. §17902.

53. The HIPAA Breach Notification Rule, 45 C.F.R. §§ 164.400-414, also requires Defendant to provide notice of the cybersecurity breach to each affected individual “without unreasonable delay and in no case later than 60-days following discovery of the breach.”

54. HIPAA requires a covered entity to have and apply appropriate sanctions against members of its workforce who fail to comply with the privacy policies and procedures of the covered entity or the requirements of 45 C.F.R. Part 164, Subparts D or E. See 45 C.F.R. § 164.530(e).

55. HIPAA requires a covered entity to mitigate, to the extent practicable, any harmful effect that is known to the covered entity of a use or disclosure of protected health information in violation of its policies and procedures or the requirements of 45 C.F.R. Part 164, Subpart E by the covered entity or its business associate. See 45 C.F.R. § 164.530(f).

56. HIPAA also requires the Office of Civil Rights (“OCR”), within the Department of Health and Human Services (“HHS”), to issue annual guidance documents on the provisions in the HIPAA Security Rule. See 45 C.F.R. §§ 164.302-164.318. For example, “HHS has developed guidance and tools to assist HIPAA covered entities in identifying and implementing the most cost effective and appropriate administrative, physical, and technical safeguards to protect the confidentiality, integrity, and availability of e-PHI and comply with the risk analysis requirements of the Security Rule.” See US Department of Health & Human Services, Security Rule Guidance Material. The list of resources includes a link to guidelines set by the National Institute of Standards and Technology (NIST), which OCR says “represent the industry standard for good

business practices with respect to standards for securing e-PHI.” See US Department of Health & Human Services, Guidance on Risk Analysis.

Defendant Breached Their Duties to Safeguard Plaintiff's and Class Members' Private Information

57. In addition to its obligations under federal and state laws, LURIE owed a duty to Plaintiff and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the Private Information in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. LURIE owed a duty to Plaintiff and Class Members to provide reasonable security to ensure that its computer systems, networks, and protocols adequately protected the Private Information of Class Members

58. LURIE breached its obligations to Plaintiff and Class Members and/or was otherwise negligent because it failed to properly maintain and safeguard its computer systems and data and failed to audit, monitor, or ensure the integrity of its vendor’s data security practices.

59. LURIE’s conduct includes, but is not limited to, the following acts and/or omissions:

- a. Failing to maintain an adequate data security system that would reduce the risk of cybersecurity breaches and cyberattacks;
- b. Failing to adequately protect its patients’ Private Information;
- c. Failing to adhere to HIPAA guidelines and industry standards for cybersecurity as discussed above; and,
- d. Otherwise breaching its duties and obligations to protect Plaintiff’s and Class Members’ Private Information.

60. LURIE negligently failed to safeguard Plaintiff’s and Class Members’ Private Information by allowing cyberthieves to access the Private Information.

61. Had LURIE's remedied the deficiencies in its information storage and security practices or those of its vendors and affiliates, and adopted security measures to prevent such a cyberattack, it could have prevented intrusion into its information storage and security systems and, ultimately, the theft of Plaintiff's and Class Members' confidential Private Information.

COMMON INJURIES & DAMAGES

62. As a result of the cybersecurity breach, and the foreseeable consequences of Private Information ending up in the possession of criminals, the risk of identity theft to the Plaintiff and Class Members has materialized, and Plaintiff and Class Members have all sustained actual injuries and damages, including: (i) invasion of privacy; (ii) theft of their Private Information; (iii) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the cybersecurity breach; (iv) lost opportunity costs associated with attempting to mitigate the actual consequences of the cybersecurity breach; (v) statutory damages; (vi) nominal damages; and (vii) the continued and certainly increased risk to their Private Information.

The Cybersecurity Breach Increases Victims' Risk of Identity Theft

63. There is high likelihood that the Private Information of Plaintiff and Class Members will end up for sale on the dark web as that is the modus operandi of hackers.

64. Private Information may also fall into the hands of companies that will use the detailed Private Information for targeted marketing without the approval of Plaintiff and Class Members. Simply, unauthorized individuals can easily access the Private Information of Plaintiff and Class Members.

65. The link between a cybersecurity attack and the risk of identity theft is simple and well established. Criminals acquire and steal Private Information to monetize the information. Criminals monetize the data by selling the stolen information on the black market to other

criminals who then utilize the information to commit a variety of identity theft related crimes discussed below.

66. The Plaintiff and Class Members' Private Information is of great value to hackers and cyber criminals, and the data stolen in the cybersecurity breach has been used and will continue to be used in a variety of sordid ways for criminals to exploit Plaintiff and Class Members and to profit off their misfortune.

67. As a result of the recognized risk of identity theft, when a Cybersecurity breach occurs, and an individual is notified by a company that their Private Information was compromised, as in this cybersecurity breach, the reasonable person is expected to take steps and spend time to address the dangerous situation, learn about the breach, and otherwise mitigate the risk of becoming a victim of identity theft or fraud. Failure to spend time taking steps to review accounts or credit reports could expose the individual to greater financial harm – yet, the resource and asset of time has been lost.

68. Therefore, due to the actual and imminent risk of identity theft, Plaintiff and Class Members must monitor their financial accounts for many years to mitigate the risk of identity theft.

69. As a result of the cybersecurity attack, Plaintiff's and Class Members' Private Information, which has an inherent market value in both legitimate and dark markets, has been damaged and diminished by its compromise and unauthorized release. However, this transfer of value occurred without any consideration paid to Plaintiff or Class Members for their property, resulting in an economic loss. Moreover, under information and belief, the Private Information is now readily available, and the rarity of the Data has been lost, thereby causing additional loss of value.

70. At all relevant times, LURIE knew, or reasonably should have known, of the importance of safeguarding the Private Information of Plaintiff and Class Members, and of the foreseeable consequences that would occur if Defendant' data security systems were breached.

71. The total consequences resulting from the Cybersecurity breach may not come to light for years.

72. LURIE was, or should have been, fully aware of the unique type and the significant volume of data on Defendant' networks, and thus, the significant number of individuals who would be harmed by cybersecurity attack.

73. The injuries to Plaintiff and Class Members were directly and proximately caused by Defendant' failure to implement or maintain adequate data security measures for the Private Information of Plaintiff and Class Members.

74. Based on the type of targeted attack in this case, sophisticated criminal activity, and the volume and type of Private Information involved, there is a strong probability that entire batches of compromised information have been placed, or will be placed, on the black market/dark web for sale and purchase by criminals intending to utilize the Private Information at the expense of the Plaintiff and Class Members.

75. Such fraud may go undetected for years. An individual may not know that his or her Private Information was used at their expense.

76. Consequently, Plaintiff and Class Members are at an increased risk of fraud and identity theft for many years into the future.

Plaintiff Foxie's Experience

77. Plaintiff, Byron Foxie who is the legal guardian and parent of Tige Foxie, admitted his son Tige Foxie into Almost Home, a LURIE facility, as a patient on and off from November, 2010 to November, 2017.

78. In order to obtain medical services from LURIE, the Plaintiff was required to provide Private Information, directly or indirectly, to Almost Home/LURIE, the Defendant.

79. The patient records, covering Tige Foxie's medical care from LURIE are electronically stored at LURIE's Chicago facility that were subject to the cybersecurity attack.

80. Tige Foxie is totally disabled, unable to do anything by himself, he is trached, vented and needs 24-hour assistance for his well being, including but not limited to suctioning and repositioning.

81. On July 8, 2019, the Plaintiff filed a lawsuit against LURIE's in the Circuit Court of Cook County, Illinois, Law Division based on negligence and spoliation of evidence among other counts.

82. The spoliation of evidence alleges LURIE's failed to "maintain/record any electronic administrative notes for the Plaintiff on November 27, 2017." And, medical records and consult notes are conspicuously missing for November 27, 2017." Quotations taken from Plaintiff's Complaint against the Defendant.

83. This civil case against the Defendant this still active and on-going. Based on this cybersecurity attack, at this time, there is no way to know how this breach will affect this separate current civil litigation undertaken by the Plaintiff against the Defendant.

84. At the time of the cybersecurity breach, Defendant retained Plaintiff's Information in their electronic systems.

85. Based on Tige Foxie's physical condition and vulnerability, the Plaintiff has to be very careful about sharing his sensitive Private Information.

86. Plaintiff suffered actual injury from having his Private Information compromised as a result of the cybersecurity attack including, but not limited to: (i) invasion of privacy; (ii) theft of their Private Information; (iii) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the cybersecurity breach; (iv) lost opportunity costs associated with attempting to mitigate the actual consequences of the cybersecurity breach; (v) statutory damages; (vi) nominal damages; and (vii) the continued and certainly increased risk to their Private Information.

87. This cybersecurity attack has caused the Plaintiff to suffer fear, anxiety, and stress, which has been compounded by the fact that LURIE has still not informed Plaintiff of any details about the cybersecurity breach's occurrence.

88. The Plaintiff has a continuing interest in ensuring that his Private Information, in addition to protecting the medical records to support the allegations in his pending civil lawsuit remain backed-up in Defendant's possession, and the Private Information is protected and safeguarded from future breaches.

CLASS ALLEGATIONS

89. The Plaintiff brings this nationwide class action on behalf of himself and on behalf of all others similarly situated pursuant to 735 ILCS 5/2—801 et seq.

90. The Class that Plaintiff seeks to represent is defined as follows:

Nationwide Class

All individuals residing in the United States whose Private Information was accessed and/or acquired by an unauthorized party in the cybersecurity breach (the "Class").

Illinois Subclass

All individuals residing in the state of Illinois whose Private Information was accessed and/or acquired by an unauthorized party in the cybersecurity breach (the “Subclass”).

91. Excluded from the Classes are the following individuals and/or entities: Defendant and Defendant’s, subsidiaries, affiliates, officers and directors, and any entity in which Defendant has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

92. Plaintiff reserves the right to amend the definitions of the Class and/or Illinois Subclass or add a Class or Subclass if further information and discovery indicate that the definitions of the Class should be narrowed, expanded, or otherwise modified.

93. Numerosity: The members in the Class are so numerous that joinder of each of the Class Members in a single proceeding would be impracticable. According to the LURIE website, more than 239,000 children medical care at LURIE Children’s each year

94. Common questions of law and fact exist as to all members of the Class and predominate over any questions affecting solely individual members of the Class. Among the questions of law and fact common to the Class that predominate over questions which may affect individual Class Members, including the following:

- a. Whether and to what extent Defendant had a duty to protect the Private Information of Plaintiff and Class Members;
- b. Whether Defendant had respective duties not to disclose the Private Information of Plaintiff and Class Members to unauthorized third parties;
- c. Whether Defendant failed to adequately safeguard the Private Information of Plaintiff and Class Members;
- d. Whether and when Defendant actually learned of the cybersecurity breach;

- FILED DATE: 2/9/2024 5:20 PM 2024CH00869
- e. Whether Defendant adequately, promptly, and accurately informed Plaintiff and Class Members that their Private Information had been compromised;
 - f. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the cybersecurity breach;
 - g. Whether Defendant adequately addressed and fixed the vulnerabilities which permitted the Cybersecurity breach to occur;
 - h. Whether Plaintiff and Class Members are entitled to actual damages, statutory damages, and/or nominal damages as a result of Defendant' wrongful conduct;
 - i. Whether Plaintiff and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Cybersecurity breach.

95. Typicality: Plaintiff's claims are typical of those of the other members of the Class because Plaintiff, like every other Class Member, was exposed to virtually identical conduct and now suffers from the same violations of the law as each other member of the Class.

96. Policies Generally Applicable to the Class: This class action is also appropriate for certification because Defendant acted or refused to act on grounds generally applicable to the Class, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members and making final injunctive relief appropriate with respect to the Class as a whole. Defendant's policies challenged herein apply to and affect Class Members uniformly and Plaintiff's challenge of these policies hinges on Defendant' conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiff.

97. Adequacy. Plaintiff will fairly and adequately represent and protect the interests of the Class Members in that he has no disabling conflicts of interest that would be antagonistic to those of the other Class Members. Plaintiff seeks no relief that is antagonistic or adverse to the Class Members and the infringement of the rights and the damages he has suffered are typical of other Class Members. Plaintiff and his counsel intend to prosecute this action vigorously.

98. Superiority and Manageability: The class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of Class Members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain Class Members, who could not individually afford to litigate a complex claim against large corporations, like Defendant. Further, even for those Class Members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

99. The nature of this action and the nature of laws available to Plaintiff and Class Members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiff and Class Members for the wrongs alleged because Defendant would necessarily gain an unconscionable advantage since they would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiff was exposed is representative of that experienced by the Class and will establish the right of each Class Member to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

100. The litigation of the claims brought herein is manageable. Defendant's uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class

Members demonstrates that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

101. Adequate notice can be given to Class Members directly using information maintained in Defendant' records.

102. Unless a Class-wide injunction is issued, Defendant may continue in its failure to properly secure the Private Information of Class Members, Defendant may continue to refuse to provide proper notification to Class Members regarding the Cybersecurity breach, and Defendant may continue to act unlawfully as set forth in this Complaint.

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

COUNT I
Negligence
(On Behalf of Plaintiff and the Class)

104. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

105. Defendant owed a duty to Plaintiff and Class Members to exercise reasonable care in safeguarding and protecting the Private Information in their possession, custody, or control.

106. Defendant knew or should have known the risks of collecting and storing Plaintiff's and all other Class Members' Private Information and the importance of maintaining secure systems. Defendant knew or should have known of the many cybersecurity breaches that targeted healthcare providers that collect and store Private Information in recent years.

107. Based the nature of cybersecurity breach, Defendant should have identified the vulnerabilities to their systems or their third-party vendor's systems and prevented the cybersecurity breach from occurring.

108. Defendant breached these duties by failing to exercise reasonable care in safeguarding and protecting Plaintiff's and Class Members' Private Information by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems to safeguard and protect Private Information entrusted to it—including Plaintiff's and Class Members' Private Information.

109. It was reasonably foreseeable to Defendant that their failure to exercise reasonable care in safeguarding and protecting Plaintiff's and Class Members' Private Information by failing to, design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems would result in the unauthorized release, disclosure, and dissemination of Plaintiff's and Class Members' Private Information.

110. But for Defendant' negligent conduct or breach of the above-described duties owed to Plaintiff and Class Members, their Private Information would not have been compromised.

111. As a result of Defendant' above-described wrongful actions, inaction, and want of ordinary care that directly and proximately caused the cybersecurity attack, Plaintiff and Class Members have suffered and will suffer injury, including, but not limited to: (i) invasion of privacy; (ii) theft of their Private Information; (iii) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the cybersecurity breach; (iv) lost opportunity costs associated with attempting to mitigate the actual consequences of the cybersecurity breach;

(v) statutory damages; (vi) nominal damages; and (vii) the continued and certainly increased risk to their Private Information.

COUNT II
Negligence Per Se
(On Behalf of Plaintiff and the Class)

112. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

113. The Defendant's duties arise from, *inter alia*, the HIPAA Privacy Rule ("Standards for Privacy of Individually Identifiable Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and E, and the HIPAA Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C (collectively, "HIPAA Privacy and Security Rules").

114. Defendant's duties also arise from Section 5 of the FTC Act ("FTCA"), 15 U.S.C. § 45(a)(1), which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted by the FTC, the unfair act or practice by business, such as LURIE, of failing to employ reasonable measures to protect and secure PII/PHI.

115. Defendant's duties also arise from the Illinois Personal Information Protection Act ("IPIPA"), 815 ILCS 530/45(a) which requires: A data collector that owns or licenses, or maintains or stores but does not own or license, records that contain personal information concerning an Illinois resident shall implement and maintain reasonable security measures to protect those records from unauthorized access, acquisition, destruction, use, modification, or disclosure. 815 ILCS. 530/45.

116. Under 815 ILCS 530/10, Defendant had a duty to "notify the resident at no charge that there has been a breach of the security of the system data following discovery or notification

of the breach [...] in the most expedient time possible and without unreasonable delay.” 815 ILCS 530/10.

117. The Defendant violated HIPAA Privacy and Security Rules, Section 5 of the FTCA, and IPIPA by failing to, or contracting with companies that failed to, use reasonable measures to protect Plaintiff’s and other Class Members’ Private Information, by failing to provide timely notice, and by not complying with applicable industry standards. Defendant’ conduct was particularly unreasonable given the nature and amount of Private Information they obtain and store, and the foreseeable consequences of a cybersecurity breach involving Private Information including, specifically, the substantial damages that would result to Plaintiff and the other Class Members.

118. Defendant’s violation of IPIPA, HIPAA Privacy and Security Rules, and Section 5 of the FTCA constitutes negligence per se.

119. Plaintiff and Class Members are within the class of persons that IPIPA, HIPAA Privacy and Security Rules, and Section 5 of the FTCA were intended to protect.

120. The harm occurring as a result of the cybersecurity breach is the type of harm that IPIPA, HIPAA Privacy and Security Rules, and Section 5 of the FTCA were intended to guard against.

121. It is reasonably foreseeable to Defendant that their failure to exercise reasonable care in safeguarding and protecting Plaintiff’s and Class Members’ Private Information by failing to, design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems, would result in the release, disclosure, and dissemination of Plaintiff’s and Class Members’ Private Information to unauthorized individuals.

122. The injury and harm that Plaintiff and the other Class Members suffered was the direct and proximate result of Defendant's violations of harm IPIPA, HIPAA Privacy and Security Rules, and Section 5 of the FTCA.

123. Plaintiff and Class Members have suffered and will suffer injury, including, but not limited to: (i) invasion of privacy; (ii) theft of their Private Information; (iii) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the cybersecurity breach; (iv) lost opportunity costs associated with attempting to mitigate the actual consequences of the cybersecurity breach; (v) statutory damages; (vi) nominal damages; and (vii) the continued and certainly increased risk to their Private Information.

COUNT III
Breach of Fiduciary Duty
(On Behalf of Plaintiff and the Class)

124. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

125. Plaintiff and Class Members gave LURIE their Private Information in confidence, believing that LURIE would protect that information.

126. Plaintiff and Class Members would not have provided LURIE with this information had they known it would not be adequately protected. LURIE's acceptance and storage of Plaintiff's and Class Members' Private Information created a fiduciary relationship between LURIE and Plaintiff and Class Members.

127. Based on this relationship, LURIE must act primarily for the benefit of its patients, which includes safeguarding and protecting Plaintiff's and Class Members' Private Information.

128. Due to the nature of the relationship between LURIE and Plaintiff and Class Members, Plaintiff and Class Members were entirely reliant upon LURIE to ensure that their

PII/PHI was adequately protected. Plaintiff and Class Members had no way of verifying or influencing the nature and extent of LURIE's or its vendors data security policies and practices, and LURIE was in an exclusive position to guard against the cybersecurity attack.

129. The Defendant has a fiduciary duty to act for the benefit of Plaintiff and Class Members upon matters within the scope of their relationship. They breached that duty by contracting with companies that failed to, properly protect the integrity of the system containing Plaintiff's and Class Members' Private Information, failing to comply with the data security guidelines set forth by HIPAA, and otherwise failing to safeguard Plaintiff's and Class Members' PII/PHI that they collected.

130. As a direct and proximate result of LURIE's breaches of its fiduciary duties, Plaintiff and Class Members have suffered and will suffer injury, including, but not limited to: (i) invasion of privacy; (ii) theft of their Private Information; (iii) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the cybersecurity breach; (iv) lost opportunity costs associated with attempting to mitigate the actual consequences of the cybersecurity breach; (v) statutory damages; (vi) nominal damages; and (vii) the continued and certainly increased risk to their Private Information.

COUNT IV
Breach of Implied Contract
(On Behalf of Plaintiff and the Class)

131. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

132. In connection with receiving healthcare services, Plaintiff and all other Class Members entered into implied contracts with LURIE.

133. Pursuant to these implied contracts, Plaintiff and Class Members paid money to LURIE, directly or through their insurance, and provided LURIE with their Private Information. In exchange, LURIE agreed to, among other things, and Plaintiff and Class Members understood that LURIE would: (1) provide services to Plaintiff and Class Members; (2) take reasonable measures to protect the security and confidentiality of Plaintiff's and Class Members' Private Information; and (3) protect Plaintiff's and Class Members' Private Information in compliance with federal and state laws and regulations.

134. The protection of Private Information was a material term of the implied contracts between Plaintiff and Class Members, on the one hand, and LURIE, on the other hand. LURIE recognized the importance of data security and the privacy of LURIE's patients' Private Information. Had Plaintiff and Class Members known that LURIE would not adequately protect their Private Information, they would not have received healthcare or other services from LURIE.

135. Plaintiff and Class Members performed their obligations under the implied contract when they provided LURIE with their Private Information and paid for healthcare or other services from LURIE.

136. LURIE breached its obligations under its implied contracts with Plaintiff and Class Members in failing to implement and maintain reasonable security measures to protect and secure their Private Information, including by ensuring companies it contracts with implement and maintain reasonable security measures to protect Private Information, and in failing to implement and maintain security protocols and procedures to protect Plaintiff's and Class Members' Private Information in a manner that complies with applicable laws, regulations, and industry standards.

137. LURIE's breach of its obligations of its implied contracts with Plaintiff and Class Members directly resulted in the cybersecurity attack and the injuries that Plaintiff and all other Class Members have suffered from the cybersecurity attack.

138. Plaintiff and all other Class Members were damaged by LURIE's breach of implied contracts because: (i) they paid—directly or through their insurers—for data security protection they did not receive; (ii) they face a substantially increased risk of identity theft and medical theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (iii) their Private Information was improperly disclosed to unauthorized individuals; (iv) the confidentiality of their Private Information has been breached; (v) they were deprived of the value of their Private Information, for which there is a well-established national and international market; (vi) lost time and money incurred to mitigate and remediate the effects of the cybersecurity attack, including the increased risks of identity theft they face and will continue to face; and (vii) overpayment for services that were received without adequate data security.

COUNT V

Unjust Enrichment (In the Alternative) (On Behalf of Plaintiff and the Class)

139. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein, with the exception of the implied contract claim.

140. This claim is pleaded in the alternative to the breach of implied contract claim.

141. Plaintiff and Class Members conferred a monetary benefit upon Defendant in the form of monies paid to LURIE for healthcare services, which LURIE used in turn to pay for different services, and through the provision of their PII/PHI.

142. Defendant accepted or had knowledge of the benefits conferred upon them by Plaintiff and Class Members. Defendant also benefitted from the receipt of Plaintiff's and Class Members' Private Information, as this was used to facilitate billing services and services provided to LURIE.

143. As a result of Defendant's conduct, Plaintiff and Class Members suffered actual damages in an amount equal to the difference in value between their payments made with reasonable data privacy and security practices and procedures that Plaintiff and Class Members paid for, and those payments without reasonable data privacy and security practices and procedures that they received.

144. Defendant should not be permitted to retain the money belonging to Plaintiff and Class Members because Defendant failed to adequately implement the data privacy and security procedures for themselves that Plaintiff and Class Members paid for and that were otherwise mandated by federal, state, and local laws and industry standards.

145. Plaintiff and Class Members have no adequate remedy at law.

146. Defendant should be compelled to provide for the benefit of Plaintiff and Class Members all unlawful proceeds received by them as a result of the conduct and cybersecurity attack alleged herein.

COUNT VI

Violations of The Illinois Consumer Fraud And Deceptive Business Practices Act,
815 ILCS 505/2, et seq.
(On Behalf of Plaintiff and the Illinois Subclass)

147. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein and brings this claim on behalf of himself and the Illinois Subclass (the "Class" for the purposes of this count).

148. Defendant offered and continues to offer healthcare or other related services in the State of Illinois.

149. Plaintiff and Class Members purchased and received healthcare or other services from Defendant for personal, family, or household purposes.

150. Defendant engaged in unlawful and unfair practices in violation of the ICFA by failing to, or contracting with companies that failed to, implement and maintain reasonable security measures to protect and secure Plaintiff's and Class Members' Private Information in a manner that complied with applicable laws, regulations, and industry standards.

151. Defendant makes explicit statements to their patients that their Private Information will remain private.

152. Defendant's duties also arise from the Illinois Personal Information Protection Act, 815 ILCS 530/45(a) which requires: A data collector that owns or licenses or maintains or stores but does not own or license, records that contain personal information concerning an Illinois resident shall implement and maintain reasonable security measures to protect those records from unauthorized access, acquisition, destruction, use, modification, or disclosure.

153. Defendant violated this duty by failing to, or contracting with companies that failed to, implement reasonably secure data security policies.

154. As of the date of filing this Class Action Complaint, the Defendant has not notified the Plaintiff of the cybersecurity attack. The Illinois Personal Information Protection Act requires entities that experience a cybersecurity breach to notify Illinois residents "in the most expedient time possible and without unreasonable delay." 815 ILCS 530/10. Violation of the Illinois Personal Information Protection Act constitutes an unlawful practice under the ICFA. 815 ILCS 530/20.

155. Due to the cybersecurity breach, Plaintiff and Class Members have lost property in the form of their PII/PHI. This breach will force Plaintiff and Class Members to spend time or money to protect against identity theft. Plaintiff and Class Members are now at a higher risk of medical identity theft and other crimes. This harm sufficiently outweighs any justifications or motives for Defendant' practice of collecting and storing Private Information without appropriate and reasonable safeguards to protect such information.

156. As a result of Defendant's' violations of the ICFA, Plaintiff and Class Members have suffered and will suffer injury, including, but not limited to: (i) invasion of privacy; (ii) theft of their Private Information; (iii) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the cybersecurity attack; (iv) lost opportunity costs associated with attempting to mitigate the actual consequences of the cybersecurity breach; (v) statutory damages; (vi) nominal damages; and (vii) the continued and certainly increased risk to their Private Information.

PRAYER FOR RELIEF

Plaintiff, individually, and on behalf of all other members of the Class, respectfully requests that the Court enter judgment in his favor and against Defendant as follows:

A. Certifying the Class as requested herein, designating Plaintiff as Class representative, and appointing Plaintiff's counsel as Class Counsel;

B. Awarding Plaintiff and the Class Members appropriate monetary relief, including actual damages, statutory damages, punitive damages, restitution, and disgorgement;

C. Awarding Plaintiff and the Class equitable, injunctive, and declaratory relief, as may be appropriate. Plaintiff, on behalf of himself and the Class, seeks appropriate injunctive relief designed to prevent Defendant from experiencing another cyber cybersecurity breach by adopting

and implementing best data security practices to safeguard Private Information and to provide or extend credit monitoring services and similar services to protect against all types of identity theft and medical identity theft;

D. Awarding Plaintiff and the Class pre-judgment and post-judgment interest to the maximum extent allowable;

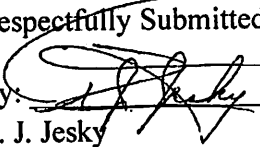
E. Awarding Plaintiff and the Class reasonable attorneys' fees, costs, and expenses, as allowable; and

F. Awarding Plaintiff and the Class such other favorable relief as allowable under law.

JURY TRIAL DEMANDED

Plaintiff hereby demands a trial by jury on all claims so triable.

Dated: February 9, 2024

Respectfully Submitted,
By: 
T. J. Jesky
Law Offices of T. J. Jesky
205. N. Michigan Ave., Suite 810
Chicago, IL 60601-5902
Phone: (312) 894-0130
Fax: (312) 489-8216
Attorney Number: 63014
tj@jeskylaw.com