☐ YES ☑ NO

EXHIBITS

CASE NO. 2022 L 2432

DATE: 3/11/2022

CASE TYPE: Commercial Litigation

PAGE COUNT: 29

CASE NOTE

_____

_____

_____

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

JANE DOE, individually and on behalf of all others similarly situated,

Plaintiff,

v.

SOUTH SHORE HOSPITAL CORPORATION,

Defendant.

Case No. 2022L002432

CLASS ACTION

JURY TRIAL DEMANDED

Hearing Date: 7/12/2022 9:00 AM

CLASS ACTION COMPLAINT

Plaintiff Jane Doe ("Jane Doe" or "Plaintiff") brings this action on behalf of herself and all others similarly situated against Defendant, South Shore Hospital Corporation (collectively, "SSH" or "Defendant"), and its present, former, or future direct and indirect parent companies, subsidiaries, affiliates, agents, and/or other related entities, and alleges as follows:

INTRODUCTION

1. SSH, an independent general acute care hospital located in the South Shore community of Chicago, failed to safeguard 115,670 patients' and employees' highly sensitive personal and medical information from cybercriminals in a security breach of its file servers in approximately December 2021 (the "Data Breach").

2. SSH serves real people and real families, like Plaintiff and Class members. Jane Doe was a SSH patient and Data Breach victim, and she brings this class action on behalf of all individuals harmed by SSH's misconduct.

3. The majority of SSH's patient population resides in the communities surrounding the hospital. The majority of the population (87%) within SSH's service area identifies as

African American/Black. Nine percent of the population identifies as Hispanic/Latinx, and 3% as non-Hispanic white. The primary patient population is geriatric with low to moderate income levels. SSH advertises that it treats patients regardless of race, color, creed, or their ability to pay.[1]

4. The top health issues in the communities served by SSH are diabetes, mental health, violence, substance-use, age-related illness, heart disease and stroke.[2] SSH offers special medical detoxification and geriatric psychiatric services to address these issues. As a result, SSH was in possession of significant stores of highly sensitive personal health information ("PHI") and personally identifying information ("PII").

5. Vulnerable people, like those with substance-abuse issues and the elderly, can make for ideal targets for scams and extortion. These are the people whose data SSH put at risk, and ultimately exposed, by using inadequate safeguards that allowed cybercriminals to bypass lax security measures to access patients' and employees' data, including first and last names, addresses, dates of birth, Social Security numbers, financial information, health insurance information, medical information, diagnoses, health insurance policy numbers, and Medicare and Medicaid information.

6. To make matters worse, following the Data Breach, SSH did not notify Plaintiff and Class members in the "most expedient time possible and without unreasonable delay," as required by Illinois law,[3] instead waiting two months to notify Plaintiff and Class members. In that time, Plaintiff and Class members were unaware of the Data Breach and unable to proactively mitigate the Data Breach's impact on them or protect their identities from theft.

---

[1] https://www.southshorehospital.com/wp-content/uploads/2019/12/FINAL-South-Shore-Hospital-Report_13November2019.pdf, at 1 (last accessed March 9, 2022).
[2] *Id.* at 8.
[3] 815 ILCS § 530/10(a).

7. On February 4, 2022, SSH posted a Notice of Cybersecurity Incident on its website: https://www.southshorehospital.com/notice-of-cybersecurity-incident/.

PARTIES

8. Plaintiff, Jane Doe, is an adult individual and Illinois citizen, residing in Calumet City, Illinois, where she intends to remain. Jane Doe was an SSH patient and Data Breach victim. On or about March 7, 2022, she confirmed with SSH that her PHI and PII were compromised as a result of the Data Breach.

9. Defendant SSH is an Illinois not-for-profit corporation headquartered at 8012 South Crandon Avenue Chicago, IL 60617, United States.

JURISDICTION & VENUE

10. This Court has subject-matter jurisdiction over this action under Ill. Const. art. VI, § 9.

11. This Court has general personal jurisdiction over SSH under 735 ILCS § 5/2-209 because it is incorporated under the laws of Illinois and headquartered in Illinois.

12. Venue is proper in this Court under 735 ILCS § 5/2-101(2) because SSH resides in Cook County and the transactions, or some part thereof out of which the cause of action arose, occurred in Cook County.

BACKGROUND FACTS

SSH

13. SSH offers general acute hospital care in the Chicago area. In so doing, SSH collects highly sensitive PII and PHI from its patients and employees. Indeed, SSH requires that patients disclose their PII and PHI in order to receive SSH's services.

14. The PII and PHI that SSH collects from patients includes first and last names, dates of birth, addresses, patient identification numbers, insurance card numbers, driver's license numbers, insurance cards, credit card numbers, and Social Security numbers. Similar PII and PHI is collected by SSH from employees.

15. When SSH collects this sensitive information, it promises to use reasonable measures to safeguard their PII and PHI from theft and misuse.

16. In fact, SSH recognizes its duty to protect data, stating "South Shore Hospital is committed to providing you with the highest quality of care in an environment that protects your privacy and the confidentiality of your medical information."[4] SSH also admits it is responsible for "[m]aintaining the privacy of your health information as required by law."[5]

17. Despite "valu[ing] the privacy and confidentiality of all patient data within its control,"[6] SSH does not follow industry standard practices in securing PII and PHI. On information and belief, SSH does not adequately train its employees on cybersecurity policies, enforce those policies, or maintain reasonable security practices and systems. Indeed, on information and belief, SSH stores PII and PHI data in multiple locations, all with differing

[4] https://www.southshorehospital.com/privacy-practices/ (last visited March 9, 2020).
[5] *Id.*
[6] https://www.southshorehospital.com/notice-of-cybersecurity-incident/ (last visited March 9, 2020).

security safeguards. As a result, SSH may adequately protect data in one system, but leave it vulnerable to extraction in another.

SSH Fails to Safeguard Plaintiff and Class members' PHI and PII

18. Jane Doe and the proposed Class are current and former SSH patients and employees.

19. As a condition to providing treatment, SSH required Jane Doe and the proposed Class to provide their PHI and PII.

20. As a condition of employment with SSH, SSH requires its employees to disclose their PII.

21. SSH then collected and maintained patient and employee PHI and PII in its computer systems.

22. In providing their PHI and PII, Jane Doe and proposed Class members reasonably expected that SSH would safeguard that sensitive information, including protecting it from unauthorized disclosure during a data breach or data leak.

23. On information and belief, SSH stored PHI and PII in multiple locations, all using different security safeguards.

24. On information and belief, SSH does not adequately train its employees on security protocols to securely maintain their credentials and access information.

25. On December 10, 2021, despite SSH's promises to safeguard patient data, "SSH became aware of unauthorized activity on its network."[7]

26. SSH states that after it discovered the breach, it activated its emergency operating protocols to ensure its facility could continue providing care to patients. SSH also hired

[7] *Id.*

"independent computer forensic experts" to investigate and determine what information was involved in the breach.[8]

27. The investigation determined that the files impacted may have contained Plaintiff and Class members' first and last names, addresses, dates of birth, Social Security numbers, financial information, health insurance information, medical information, diagnoses, health insurance policy numbers, and Medicare/Medicaid information.[9]

28. After the breach, SSH implemented "additional security controls to protect [its] network," including "enforcing stronger password requirements, enabling multifactor authentication, and additional data privacy and security awareness training for SSH's workforce."[10] SSH also "deployed supplementary anti-malware and email phishing tools."[11] These are safeguards that should have been in place *before* the Data Breach.

29. SSH did not immediately notify the government or victims of the Data Breach about the Data Breach and instead waited two months before issuing its breach notice ("Breach Notice").

30. On February 4, 2022, SSH posted a Notice of Cybersecurity Incident on its website: https://www.southshorehospital.com/notice-of-cybersecurity-incident/.

31. On February 7, 2022, SSH disclosed to the U.S. Department of Health and Human Services ("HHS") that its network server was hacked. As required by section 13402(e)(4) of the HITECH Act, the Secretary must post a list of breaches of unsecured protected health information affecting 500 or more individuals. SSH's breach was included in the Secretary's list.

[8] *Id.*
[9] *Id.*
[10] *Id.*
[11] *Id.*

32. SSH offered "identity theft protection services through IDX, a data breach and recovery services expert, at no charge to SSH patients affected. These services include 12 months of credit and CyberScan monitoring, a $1,000,000 insurance reimbursement policy, and fully managed identity theft recovery services."[12]

Plaintiff's Experience

33. Jane Doe is a former SSH patient.

34. As a condition of receiving SSH's services, SSH required Jane Doe to provide her PHI and PII, and Jane Doe indeed provided SSH with her PHI and PII as part of receiving SSH's services.

35. On or about March 7, 2022, Jane Doe called the toll-free number, 1-833-783-1445, as instructed by SSH in its Breach Notice, and became aware that her PHI and PII were compromised in the Data Breach. She was told SSH would provide her with credit monitoring, and she enrolled in that protection.

36. Jane Doe will have to spend considerable time and effort over the coming years monitoring her accounts to protect herself from identity theft. Jane Doe's personal financial security has been jeopardized and there is uncertainty over what medical information was revealed in the Data Breach.

37. Further, Jane Doe is unsure what has happened to her PII and PHI as SSH has been unwilling to disclose the true nature of the Data Breach.

38. Had Jane Doe known that SSH does not adequately protect PII and PHI, she would not have transacted with SSH. Jane Doe would continue to transact with and utilize SSH's services, but she will not do so unless SSH takes immediate measures to ensure the data security

[12] *Id.*

of patient PII and PHI. Furthermore, Jane Doe's sensitive PII and PHI remains in SSH's possession without adequate protection against known threats, exposing Jane Doe to the prospect of additional harm in the event SSH suffers another data breach.

Jane Doe and the Proposed Class Face Significant Risk of Identity Theft

39. Jane Doe and members of the proposed Class have suffered injury from the misuse of their PII and PHI that can be directly traced to SSH.

40. The ramifications of SSH's failure to keep Plaintiff and the Class's PII and PHI secure are severe. Identity theft occurs when someone uses another's personal and financial information such as that person's name, account number, Social Security number, driver's license number, date of birth, or other information, without permission, to commit fraud or other crimes.

41. According to experts, one out of four data breach notification recipients become a victim of identity fraud.

42. Because SSH failed to prevent the Data Breach, Jane Doe and the proposed Class have suffered and will continue to suffer damages, including monetary losses and lost time. They have also suffered or are at an increased risk of suffering:

a. The loss of the opportunity to control how their PII and PHI are used;

b. The diminution in value of their PII and PHI;

c. The compromise and continuing publication of their PII and PHI;

d. Out-of-pocket costs associated with the prevention, detection, recovery, and remediation from identity theft or fraud;

e. Lost opportunity costs and lost wages associated with the time and effort expended addressing and trying to mitigate the actual and future consequences of

the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest, and recover from identity theft and fraud;

f. Delay in receipt of tax refund monies;

g. Unauthorized use of stolen PII and PHI; and

h. The continued risk to their PII and PHI, which remains in the possession of SSH and is subject to further breaches so long as SSH fails to undertake the appropriate measures to protect the PII and PHI in their possession.

43. Sensitive PII and PHI are a valuable property right. There is a burgeoning marketplace for stolen PII and PHI and a well-established illegal market for the sale and purchase of this sensitive data. Stolen PII and PHI is one of the most valuable commodities on the criminal information black market. According to Experian, a credit-monitoring service, stolen PHI can be worth up to $1,000.00 depending on the type of information obtained.

44. The value of Plaintiff's and the proposed Class's PII and PHI on the black market is considerable. Stolen PII and PHI trades on the black market for years, and criminals often post stolen private information openly on various "dark web" internet websites making the information publicly available, for a fee.

45. It can take victims years to spot identity or PII and PHI theft, giving criminals time to sell that information for cash.

46. One such example of criminals using PII and PHI for profit is the development of "Fullz" packages.

47. Cybercriminals can cross-reference multiple sources of PII and PHI to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete

scope and degree of accuracy to assemble complete dossiers on individuals. These dossiers are known as "Fullz" packages.[13]

48. The development of "Fullz" packages means that stolen PII and PHI from the Data Breach can easily be used to link and identify it to Plaintiff's and the proposed Class's phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the PII and PHI stolen by the cybercriminals in the Data Breach, criminals can easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over. That is exactly what is happening to Plaintiff and members of the proposed Class, and it is reasonable for any trier of fact, including this Court or a jury, to find that Plaintiff's and other members of the proposed Class's stolen PII and PHI is being misused, and that such misuse is fairly traceable to the Data Breach.

49. According to the FBI's Internet Crime Complaint Center (IC3) 2019 Internet Crime Report, Internet-enabled crimes reached their highest number of complaints and dollar losses that year, leading to more than $3.5 billion in losses to individuals and business victims.

50. Further, according to the same report, "rapid reporting can help law enforcement stop fraudulent transactions before a victim loses the money for good." SSH did not rapidly report to Plaintiff, the Class, or HHS that patient and employee PII and PHI had been stolen.

51. Victims of identity theft also often suffer embarrassment, blackmail, or harassment in person or online, and experience financial losses resulting from fraudulently opened accounts or misuse of existing accounts.

[13] *See* Here's How Much Your Personal Information Is Selling for on the Dark Web, Experian, https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last visited March 2, 2022).

52. Along with out-of-pocket expenses that can exceed thousands of dollars for the victim of new account identity theft, some victims must spend a considerable time repairing the damage caused by the theft of their PII and PHI. Victims of new account identity theft will likely have to spend time correcting fraudulent information in their credit reports and continually monitor their reports for future inaccuracies, close existing bank/credit accounts, open new ones, and dispute charges with creditors.

53. Further complicating the issues faced by victims of identity theft, data thieves may wait years before trying to use the stolen PII and PHI. To protect themselves, victims of data breaches, such as Jane Doe and the Class, need to remain vigilant against unauthorized data use for years or even decades to come.

54. The Federal Trade Commission ("FTC") has also recognized that consumer data is a new and valuable form of currency. In an FTC roundtable presentation, former Commissioner, Pamela Jones Harbour, stated that "most consumers cannot begin to comprehend the types and amount of information collected by businesses, or why their information may be commercially valuable. Data is currency."

55. The FTC has also issued several guidelines for businesses that highlight reasonable data security practices. The FTC has noted the need to factor data security into all business decision-making. According to the FTC, data security requires: (1) encrypting information stored on computer networks; (2) retaining payment card information only as long as necessary; (3) properly disposing of personal information that is no longer needed; (4) limiting administrative access to business systems; (5) using industry-tested and accepted methods for securing data; (6) monitoring activity on networks to uncover unapproved activity; (7) verifying

that privacy and security features function properly; (8) testing for common vulnerabilities; and (9) updating and patching third-party software.

56. According to the FTC, unauthorized PHI disclosures are extremely damaging to consumers' finances, credit history, and reputation, and can take time, money, and patience to resolve the fallout. The FTC treats the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5(a) of the FTC Act.

57. To that end, the FTC has issued orders against businesses that failed to employ reasonable measures to secure sensitive payment card data. *See In the matter of Lookout Services, Inc.*, No. C-4326, ⁋ 7 (June 15, 2011) ("[Defendant] allowed users to bypass authentication procedures" and "failed to employ sufficient measures to detect and prevent unauthorized access to computer networks, such as employing an intrusion detection system and monitoring system logs."); *In the matter of DSW, Inc.*, No. C-4157, ⁋ 7 (Mar. 7, 2006) ("[Defendant] failed to employ sufficient measures to detect unauthorized access."); *In the matter of The TJX Cos., Inc.*, No. C-4227 (Jul. 29, 2008) ("[R]espondent stored . . . personal information obtained to verify checks and process unreceipted returns in clear text on its in-store and corporate networks[,]" "did not require network administrators . . . to use different passwords to access different programs, computers, and networks[,]" and "failed to employ sufficient measures to detect and prevent unauthorized access to computer networks . . ."); *In the matter of Dave & Buster's Inc.*, No. C-4291 (May 20, 2010) ("[Defendant] failed to monitor and filter outbound traffic from its networks to identify and block export of sensitive personal information without authorization" and "failed to use readily available security measures to limit

access between instore networks . . ."). These orders, which all preceded the Data Breach, further clarify the measures businesses must take to meet their data security obligations.

CLASS ACTION ALLEGATIONS

58. Plaintiff brings this action on behalf of a class of all other persons or entities similarly situated in the state of Illinois (the "Class").

59. The Class of persons Plaintiff proposes to represent are tentatively defined as:

> All citizens of the state of Illinois whose PHI and PII was compromised in the Data Breach disclosed by SSH.

60. Excluded from the Class are counsel, SSH, any entities in which SSH has a controlling interest, any judge to whom this action is assigned, and any member of such judge's staff and immediate family.

61. The Class defined above is identifiable through SSH's business records.

735 ILCS § 5/2-801(1) Numerosity

62. There are approximately 115,670 potential Class members.

63. Individual joinder of these persons is impracticable.

64. Plaintiff is a member of the Class.

735 ILCS § 5/2-801(2) Commonality & Predominance

65. There are questions of law and fact common to Plaintiff and to the proposed Class, including but not limited to the following:

a. Whether SSH had a duty to use reasonable care in safeguarding Jane Doe's and the Class's PII and PHI;

b. Whether SSH failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

c. Whether SSH was negligent in maintaining, protecting, and securing PII and PHI;

d. Whether SSH breached contract promises to safeguard Jane Doe's and the Class's PII and PHI;

e. Whether SSH took reasonable measures to determine the extent of the Data Breach after discovering it;

f. Whether SSH's Breach Notice was reasonable;

g. Whether SSH's Breach Notice was sufficient to notify Jane Doe and the Class of the Data Breach;

h. Whether the Data Breach caused Jane Doe and the Class injuries;

i. What the proper damages measure is;

j. Whether SSH violated the statutes alleged in this Complaint; and

k. Whether Jane Doe and the Class are entitled to damages, treble damages, or injunctive relief.

66. Common questions of law and fact predominate over questions affecting only individual class members, and a class action is the superior method for fair and efficient adjudication of the controversy.

67. Plaintiff's claims are typical of the claims of Class members.

735 ILCS 5/2-801(3) Adequacy

68. Plaintiff is an adequate representative of the Class because her interests do not conflict with the interests of the Class, she will fairly and adequately protect the interests of the Class, and she is represented by counsel skilled and experienced in class actions.

735 ILCS 5/2-801(4) Appropriateness

69. The likelihood that individual members of the Class will prosecute separate actions is remote due to the time and expense necessary to prosecute an individual case.

70. Plaintiff is not aware of any litigation concerning this controversy already commenced by others who meet the criteria for class membership described above.

FIRST CLAIM FOR RELIEF
Negligence
(On Behalf of Plaintiff and the Class)

71. Plaintiff incorporates all previous paragraphs as if fully set forth below.

72. Plaintiff and members of the Class entrusted their PII and PHI to Defendant. Defendant owed to Plaintiff and other members of the Class a duty to exercise reasonable care in handling and using the PII and PHI in its care and custody, including implementing industry-standard security procedures sufficient to reasonably protect the information from the Data Breach, theft, and unauthorized use that came to pass, and to promptly detect attempts at unauthorized access.

73. Defendant owed a duty of care to Plaintiff and members of the Class because it was foreseeable that Defendant's failure to adequately safeguard their PII and PHI in accordance with state-of-the-art industry standards for data security would result in the compromise of that PII and PHI—just like the Data Breach that ultimately came to pass. Defendant acted with wanton and reckless disregard for the security and confidentiality of Plaintiff's and members of

the Class's PII and PHI by disclosing and allowing access to PII and PHI to unknown third parties and by failing to properly supervise both the way the PII and PHI was stored, used, and exchanged, and those in its employ who made that happen.

74. Moreover, Defendant owed Plaintiff and the Class a fiduciary duty of confidentiality, as Defendant provided medical treatment to the patients affected by the Data Breach or was the employer of the employees affected.

75. Defendant owed to Plaintiff and members of the Class a duty to notify them within a reasonable time frame of any breach to the security of their PII and PHI. Defendant also owed a duty to timely and accurately disclose to Plaintiff and members of the Class the scope, nature, and occurrence of the Data Breach. This duty is required and necessary for Plaintiff and members of the Class to take appropriate measures to protect their PII and PHI, to be vigilant in the face of an increased risk of harm, and to take other necessary steps to mitigate the harm caused by the Data Breach.

76. Defendant owed these duties to Plaintiff and members of the Class because they are members of a well-defined, foreseeable, and probable class of individuals whom Defendant knew or should have known would suffer injury-in-fact from Defendant's inadequate security protocols. Defendant actively sought and obtained Plaintiff's and members of the Class's PII and PHI for medical treatment services and for employment. Plaintiff and members of the Class needed to provide their PII and PHI to Defendant, (1) as patients, to receive medical treatment and services from Defendant, and (2) as prospective employees or as a condition of employment. Defendant negligently retained this information.

77. The risk that unauthorized persons would try to gain access to the PII and PHI and misuse it was foreseeable. Given that Defendant holds vast amounts of PII and PHI, it was

inevitable that unauthorized individuals would try to access Defendant's databases containing the PII and PHI—whether by malware or otherwise.

78. PII and PHI is highly valuable, and Defendant knew, or should have known, the risk in obtaining, using, handling, emailing, and storing the PII and PHI of Plaintiff and members of the Class and the importance of exercising reasonable care in handling it.

79. Defendant breached its duties by failing to exercise reasonable care in supervising its agents, contractors, vendors, and suppliers, and in handling and securing the personal information, PII, and PHI of Plaintiff and members of the Class which actually and proximately caused the Data Breach and Plaintiff's and members of the Class's injury.

80. Defendant also breached its duties by failing to provide reasonably timely notice of the Data Breach to Plaintiff and members of the Class, which actually and proximately caused and exacerbated the harm from the Data Breach and Plaintiff's and members of the Class's injuries-in-fact.

81. As a direct and traceable result of Defendant's negligence or negligent supervision, Plaintiff, and members of the Class have suffered or will suffer damages, including but not limited to monetary damages, loss of privacy, lost time, loss of value of PII and PHI, increased risk of future harm, and other damages.

82. Defendant's breach of its common-law duties to exercise reasonable care and its failures and negligence actually and proximately caused Plaintiff's and members of the Class's actual, tangible, injury-in-fact and damages, including, without limitation, the theft of their PII and PHI by criminals, improper disclosure of their PII and PHI, lost benefit of their bargain, lost value of their PII and PHI, and lost time and money incurred to mitigate and remediate the

effects of the Data Breach that resulted from and were caused by Defendant's negligence, which injury-in-fact and damages are ongoing, imminent, immediate, and which they continue to face.

83. Moreover, pursuant to the FTC Act, 15 U.S.C. § 45, Defendant has a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiff's and members of the Class's PII.

84. The FTC publications and orders promulgated pursuant to the FTC Act also form part of the basis of Defendant's duty to protect Plaintiff and the members of the Class's sensitive PII and PHI. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect customers or, in this case, patients' and employees' PII and PHI.

85. Defendant violated its duty under Section 5 of the FTC Act by failing to use reasonable measures to protect its patients' and employees' PII and PHI and not complying with applicable industry standards as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of PII and PHI Defendant had collected and stored and the foreseeable consequences of a data breach, including, specifically, the immense damages that would result to its patients and employees in the event of a breach, which ultimately came to pass.

86. The harm that has occurred is the type of harm the FTC Act is intended to guard against. Indeed, the FTC has pursued numerous enforcement actions against businesses that, because of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and members of the Class.

87. Defendant had a duty to Plaintiff and the members of the Class to implement and maintain reasonable security procedures and practices to safeguard Plaintiff's and the Class's PII.

88. Defendant breached its respective duties to Plaintiff and members of the Class under the FTC Act by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and members of the Class's PII and PHI.

89. Defendant's violation of Section 5 of the FTC Act and its failure to comply with applicable laws and regulations constitutes negligence per se.

90. But for Defendant's wrongful and negligent breach of its duties owed to Plaintiff and members of the Class, Plaintiff and members of the Class would not have been injured.

91. The injury and harm suffered by Plaintiff and members of the Class were the reasonably foreseeable result of Defendant's breach of their duties. Defendant knew or should have known that Defendant was failing to meet its duties and that its breach would cause Plaintiff and members of the Class to suffer the foreseeable harms associated with the exposure of their PII and PHI.

92. Had Plaintiff and members of the Class known that Defendant did not adequately protect the PII and PHI entrusted to it, Plaintiff and members of the Class would not have entrusted Defendant with their PII and PHI.

93. As a direct and proximate result of Defendant's negligence per se, Plaintiff and members of the Class have suffered harm, including loss of time and money resolving fraudulent charges; loss of time and money obtaining protections against future identity theft; financial losses related to the treatment Plaintiff and members of the Class paid for that they would not have sought had they known of Defendant's careless approach to cyber security; lost control over the value of PII and PHI; unreimbursed losses relating to fraudulent charges; losses relating to

exceeding credit and debit card limits and balances; harm resulting from damaged credit scores and information; and other harm resulting from the unauthorized use or threat of unauthorized use of stolen personal information, entitling them to damages in an amount to be proven at trial.

SECOND CLAIM FOR RELIEF
Breach of Implied Contract
(On Behalf of Plaintiff and the Class)

94. Plaintiff incorporates all previous paragraphs as if fully set forth below.

95. Defendant offered to provide goods and services to Plaintiff and members of the Class who were patients in exchange for payment.

96. Defendant required Plaintiff and the members of the Class to provide Defendant with their PII and/or PHI to receive services and/or as a condition of their employment.

97. In turn, Defendant agreed it would not disclose the PII and PHI it collects from patients and employees to unauthorized persons. Defendant also impliedly promised to maintain safeguards to protect the PII and PHI entrusted to it. Indeed, SSH stated that that it "is committed to providing you with the highest quality of care in an environment that protects your privacy and the confidentiality of your medical information," and that it is responsible for "[m]aintaining the privacy of your health information as required by law."

98. Plaintiff and the members of the Class who are patients accepted Defendant's offer by providing PII and PHI to Defendant in exchange for receiving Defendant's goods and services and then by paying for and receiving the same.

99. Class members who are employees accepted Defendant's offer of employment by providing their PII and PHI to Defendant.

100. Implicit in the parties' agreement was that Defendant would provide Plaintiff and members of the Class with prompt and adequate notice of all unauthorized access or theft of their PII and PHI.

101. Plaintiff and the members of the Class would not have entrusted their PII and PHI to Defendant without such agreement with Defendant.

102. Defendant materially breached the contracts it had entered with Plaintiff and members of the Class by failing to safeguard such information and failing to notify them promptly of the intrusion into its computer systems that compromised such information. Defendant also breached the implied contracts with Plaintiff and members of the Class by:

a. Failing to properly safeguard and protect Plaintiff's and members of the Class's PII and PHI;

b. Violating industry standards as well as legal obligations that are necessarily incorporated into the parties' agreement; and

c. Failing to ensure the confidentiality and integrity of electronic PII and PHI that Defendant created, received, maintained, and transmitted.

103. The damages sustained by Plaintiff and members of the Class as described above were the direct and proximate result of Defendant's material breaches of its agreements.

104. Plaintiff and members of the Class have performed under the relevant agreements, or such performance was waived by the conduct of Defendant.

105. The covenant of good faith and fair dealing is an element of every contract. All such contracts impose on each party a duty of good faith and fair dealing. The parties must act with honesty in fact in the conduct or transactions concerned. Good faith and fair dealing, in connection with executing contracts and discharging performance and other duties according to

their terms, means preserving the spirit—not merely the letter—of the bargain. Put differently, the parties to a contract are mutually obligated to comply with the substance of their contract along with its form.

106. Subterfuge and evasion violate the obligation of good faith in performance even when an actor believes their conduct to be justified. Bad faith may be overt or may consist of inaction, and fair dealing may require more than honesty.

107. Defendant failed to advise Plaintiff and members of the Class of the Data Breach promptly and sufficiently.

108. In these and other ways, Defendant violated its duty of good faith and fair dealing.

109. Plaintiff and members of the Class have sustained damages because of Defendant's breaches of its agreement, including breaches of it through violations of the covenant of good faith and fair dealing.

110. Plaintiff, on behalf of herself and the Class, seeks compensatory damages for breach of implied contract, which include, but are not limited to, the lost benefit of their bargain with SSH and the costs of future monitoring of their credit history for identity theft and fraud, plus prejudgment interest, and costs.

THIRD CAUSE OF ACTION
Unjust Enrichment
(On Behalf of the Plaintiff and the Class)

111. Plaintiff incorporates all previous paragraphs as if fully set forth below.

112. This claim is plead in the alternative to the breach of implied contractual duty claim.

113. Plaintiff and members of the Class conferred a benefit upon Defendant in the form of monies paid for treatment services and through employment.

114. Defendant appreciated or knew about the benefits conferred upon itself by Plaintiff and members of the Class. Defendant also benefited from the receipt of Plaintiff's and members of the Class's PII and PHI, as this was used to facilitate employment processing, payroll, and patient payment and treatment services.

115. Under principals of equity and good conscience, Defendant should not be permitted to retain the full value of Plaintiff and the proposed Class's services, payments, and their PII and PHI because Defendant failed to adequately protect their PII and PHI. Plaintiff and the proposed Class would not have provided their PII and PHI had they known Defendant would fail to implement (or adequately implement) appropriate data privacy and security practices and procedures that were mandated by federal, state, and local laws, and industry standards.

116. Defendant should be compelled to disgorge into a common fund to benefit Plaintiff and members of the Class all unlawful or inequitable proceeds received by it as a result of the conduct and Data Breach alleged here.

FOURTH CLAIM FOR RELIEF
Violation of Illinois Consumer Fraud and Deceptive Business Practices Act
815 ILCS § 505/1 *et seq*.
(On Behalf of the Plaintiff and the Class)

117. Plaintiff incorporates all previous paragraphs as if fully set forth below.

118. The Illinois Personal Information Protection Act ("IPIPA"), 815 ILCS § 530/20 provides that a violation of that statute constitutes an unlawful practice under the Illinois Consumer Fraud and Deceptive Business Practices Act, 815 ILCS 505/1 § *et seq.* ("ICFA"), which prohibits unfair and deceptive acts or practices in the conduct of trade and commerce.

119. Defendant is a "data collector" under IPIPA. As a data collector, Defendant owns or licenses information concerning Illinois residents.

120. The IPIPA requires a data collector that "maintains or stores . . . records that contain personal information concerning an Illinois resident shall implement and maintain reasonable security measures to protect those records from unauthorized access, acquisition, . . . use, . . . or disclosure." IPIPA, 815 ILCS § 530/45(a).

121. The IPIPA further requires that data collectors "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. The disclosure notification shall be made in the most *expedient* time possible and *without unreasonable delay*, consistent with any measures necessary to determine the scope of the breach and restore the reasonable integrity, security, and confidentiality of the data system." (emphasis added).

122. As alleged above, Defendant violated the IPIPA by failing to implement and maintain reasonable security measures to protect Plaintiff and the Class's PHI and PII. Defendant further violated the IPIPA by failing to give Plaintiff and the Class expedient notice without unreasonable delay.

123. As a direct and proximate cause of Defendant's failures, Plaintiff and the Class have suffered actual damages.

124. Plaintiff, on behalf of herself and the Class, seeks compensatory damages for breach of the IPIPA and the ICFA, which include, but are not limited to, the costs of future monitoring of their credit history for identity theft and fraud, plus attorney's fees, prejudgment interest, and costs.

FIFTH CLAIM FOR RELIEF
Breach of Fiduciary Duty
(On Behalf of the Plaintiff and the Class)

125. Plaintiff incorporates all previous paragraphs as if fully set forth below.

126. Defendant owed a fiduciary duty to Plaintiff and the Class to protect their private and sensitive PHI and PII and keep them apprised of when that information becomes exposed or compromised in a timely manner.

127. Defendant breached that fiduciary duty by, *inter alia*, failing to comply with the guidelines outlined under the Health Insurance Portability and Accountability Act ("HIPAA") and the FTC Act for safeguarding and storing it. This failure resulted in the Data Breach that ultimately came to pass.

128. Defendant further breached its fiduciary duty by failing to dispose of PHI and PII that was no longer required to render care, which unnecessarily exposed additional patients—including Plaintiff—to the Data Breach, and by failing to timely and accurately inform Plaintiff and the Class of the Data Breach which materially impaired their mitigation efforts.

129. As a direct and proximate cause of Defendant's breaches of its fiduciary duty, Plaintiff and the Class have suffered and will suffer injury, including but not limited to: (a) the compromise, publication, theft, and /or unauthorized use of their PII and PHI; (b) out-of-pocket costs associated with the prevention, detection, recovery, and remediation from identity theft and fraud; (c) lost opportunity costs and lost wages associated with efforts expended and the loss of productivity from addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft and fraud; (d) the continued risk to their PII and PHI, which remains in the possession of Defendant and is subject to further breaches so long as Defendant fails to undertake appropriate measures to protect PII and PHI in its possession; and (e) current and future costs in terms of time, effort, and money that will be

expended to prevent, detect, contest, remediate, and repair the impact of the Data Breach for the remainder of the lives of Plaintiff and the Class.

130. Plaintiff, on behalf of herself and the Class, seeks compensatory damages for breach of fiduciary duty.

SIXTH CLAIM FOR RELIEF
Invasion of Privacy
(On Behalf of the Plaintiff and the Class)

131. Plaintiff incorporates all previous paragraphs as if fully set forth below.

132. Plaintiff and the Class had a legitimate expectation of privacy regarding their highly sensitive and confidential PII and PHI and were accordingly entitled to the protection of this information against disclosure to unauthorized third parties.

133. Defendant owed a duty to Plaintiff and the Class to keep this information confidential.

134. The unauthorized acquisition (*i.e.*, theft) by a third party of Plaintiff's and Class Members' PHI and PII is highly offensive to a reasonable person.

135. The intrusion was into a place or thing which was private and entitled to be private. Plaintiff and the Class disclosed their sensitive and confidential medical information to Defendant as part of Defendant's treatments and employment, but did so privately, with the intention that their information would be kept confidential and protected from unauthorized disclosure. Plaintiff and the Class were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization.

136. The Data Breach constitutes an intentional interference with Plaintiff's and the Class's interest in solitude or seclusion, either as to their person or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

137. Defendant acted with a knowing state of mind when it permitted the Data Breach because it knew its information security practices were inadequate.

138. Defendant acted with a knowing state of mind when it failed to notify Plaintiff and the Class in a timely fashion about the Data Breach, thereby materially impairing their mitigation efforts.

139. Acting with knowledge, Defendant had notice and knew that its inadequate cybersecurity practices would cause injury to Plaintiff and the Class.

140. As a proximate result of Defendant's acts and omissions, the private and sensitive PHI and PII of Plaintiff and the Class were stolen by a third party and is now available for disclosure and redisclosure without authorization, causing Plaintiff and the Class to suffer damages.

141. Unless and until enjoined and restrained by order of this Court, Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiff and the Class since their PII and PHI are still maintained by Defendant with their inadequate cybersecurity system and policies.

142. Plaintiff and the Class have no adequate remedy at law for the injuries relating to Defendant's continued possession of their sensitive and confidential medical records. A judgment for monetary damages will not end Defendant's inability to safeguard the PII and PHI of Plaintiff and the Class.

143. In addition to injunctive relief, Plaintiff, on behalf of herself and the other members of the Class, also seeks compensatory damages for Defendant's invasion of privacy, which include, but are not limited to, the value of the privacy interest invaded by Defendant, the

costs of future monitoring of their credit history for identity theft and fraud, plus prejudgment interest, and costs.

PRAYER FOR RELIEF

Plaintiff and members of the Class demand a jury trial on all claims so triable and request that the Court enter an order:

A. Certifying this case as a class action on behalf of Jane Doe and the proposed Class, appointing Jane Doe as class representative, and appointing her counsel to represent the Class;

B. Awarding declaratory and other equitable relief as is necessary to protect the interests of Jane Doe and the Class;

C. Awarding injunctive relief as is necessary to protect the interests of Jane Doe and the Class;

D. Enjoining SSH from further deceptive and unfair practices and making untrue statements about the Data Breach and the stolen PHI and PII;

E. Awarding Jane Doe and the Class damages that include compensatory, exemplary, punitive damages, and statutory damages, including pre- and post-judgment interest, in an amount to be proven at trial;

F. Awarding restitution and damages to Plaintiff and the Class in an amount to be determined at trial;

G. Awarding attorneys' fees and costs, as allowed by law;

H. Granting Plaintiff and the Class leave to amend this complaint to conform to the evidence produced at trial; and

I. Granting such other or further relief as may be appropriate under the circumstances.

JURY DEMAND

Plaintiff demands a trial by jury on all issues so triable.

Dated: March 11, 2022

Respectfully submitted,

By: */s/Kevin J. Conway*

Kevin Conway, Esq. (ARDC #0506516)
COONEY AND CONWAY
120 North LaSalle St., 30th Floor
Chicago, IL 60602
(312) 236-6166
kconway@cooneyconway.com

Samuel J. Strauss
sam@turkestrauss.com
Raina C. Borrelli
raina@turkestrauss.com
Brittany Resch
brittanyr@turkestrauss.com
TURKE & STRAUSS LLP
613 Williamson St., Suite 201
Madison, WI 53703
Telephone (608) 237-1775
Facsimile: (608) 509-4423

J. Gerard Stranch, IV (ARDC #6334061)
Peter J. Jannace*
BRANSTETTER, STRANCH & JENNINGS, PLLC
223 Rosa L Parks Avenue, Suite 200
Nashville, TN 37203
Phone: (615) 254-8801
Fax: (615) 255-5419
gerards@bsjfirm.com
petej@bsjfirm.com

Lynn A. Toops*
COHEN & MALAD, LLP
One Indiana Square, Suite 1400
Indianapolis, Indiana 46204
(317) 636-6481
ltoops@cohenandmalad.com

Attorneys for Plaintiff and the Proposed Class

*To seek admission *pro hac vice*

ClassAction.org