12-Person Jury

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

KRISTEN MONEGATO, individually and on behalf of all others similarly situated, Plaintiff, v. FERTILITY CENTERS OF ILLINOIS, PLLC Defendant.	Case No. 2022CH00810 CLASS ACTION JURY TRIAL DEMANDED

CLASS ACTION COMPLAINT

Plaintiff Kristen Monegato ("Ms. Monegato" or "Plaintiff") brings this action on behalf of herself and all others similarly situated against Defendant, Fertility Centers of Illinois, PLLC ("FCI" 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. FCI, a fertility clinic system based in northern Illinois, lost control over its patients' highly sensitive personal and medical information to cybercriminals in a security breach ("Data Breach") and then concealed the breach from them for over ten months. When FCI finally disclosed the Data Breach, FCI misrepresented its scope and downplayed the threat it posed to patients, falsely representing that cybercriminals had not accessed patient medical records systems. The Data Breach's victims include nearly 80,000 patients seeking fertility resources and care, who disclosed their highly sensitive medical and personal information, expecting that FCI would safeguard it and timely warn them of security breaches. FCI violated those duties and Illinois law.

Ms. Monegato is an FCI patient and Data Breach victim and brings this class action on behalf of all patients harmed by FCI's misconduct.

2. FCI operates a for-profit fertility clinic system in northern Illinois, offering services like infertility treatment—such as In Vitro fertilization and surgical procedures—and fertility preservation, such as egg freezing. FCI requires that its patients disclose highly sensitive information to receive these services, including their personal health information ("PHI") and personally identifiable information ("PII"). In turn, FCI promises patients that it will "Maintain the privacy of [their] health information," and "Where required by law, notify [them] in the event that there has been a breach of [their] unsecured health information."[1]

3. In February 2021, FCI "became aware of suspicious activity on its internal systems," learning that cybercriminals had breached its systems and accessed its "administrative files," and "folders containing certain data." For the following six months, FCI did not disclose that hackers had breached its systems, choosing instead to "investigate" the breach internally.

4. On information and belief, cybercriminals were able to easily bypass FCI's systems by using an administrative account, giving them high-level access to FCI's files and wide-ranging patient data.

5. On information and belief, FCI violates industry-standard medical records retention policies by storing sensitive patient PHI and PII in several locations, leaving the data protected in some systems but an unguarded target in others. FCI's systems were inadequate and unable to prevent, detect, and stop the unauthorized hack before cybercriminal's pilfered its patient data.

6. In August 2021, FCI's six-month "investigation" revealed that cybercriminals had not only accessed administrative files and "folders containing certain data," but had, in fact,

[1] *See* FCI's Privacy Policy, https://www.fcionline.com/privacy-policy. (last visited Jan. 21, 2022).

accessed vast amounts of patient PHI and PII, including, patient names, employer assigned identification numbers, passport numbers, Social Security numbers, financial account information, payment card information, treatment information, diagnosis, treating/referring physicians, medical record number, medical billing/claims information, prescription/medication information, Medicare/Medicaid identification information, health insurance group numbers, health insurance subscriber numbers, patient account numbers, encounter numbers, ill health / retirement information, master patient index, occupational-health related information, other medical benefits and entitlements information, other medical identification numbers, patkeys/reason for absence, sickness certificate, usernames and passwords with PINs or account login information, and medical facilities associated with patient information.

7. On learning of this disturbing breach, FCI again failed to immediately warn patients and regulators that it lost control over patient PHI and PII, inexplicably waiting another four months to notify them.

8. In December 2021, FCI finally disclosed the Data Breach to the U.S. Department of Health and Human Services and notified its patients by letter ("Breach Notice").

9. FCI's Breach Notice misrepresented the nature of the breach and the threat it posed to patients. The Breach Notice informed patients that "an unauthorized third party" had accessed its systems and patient data. But the Breach Notice misrepresented, in underlined and bold-faced type, that "**no EMR (electronic medical records) systems were access or otherwise compromised as a result of this incident**." Still, the Breach Notice's following paragraph made clear that cybercriminals had accessed patients' electronically stored medical records, including "treatment information, diagnosis, treating/referring physicians, medical record number, medical

billing/claims information, prescription/medication information, master patient index, [and] occupational-health related information[.]"

10. FCI's failures to protect patients' sensitive PHI and PII—including private information about their fertility treatment and pregnancy planning—and warn them promptly and fully about the Data Breach violates Illinois law and harms tens of thousands of patients, causing Ms. Monegato to seek relief on a class wide basis.

PARTIES

11. Plaintiff, Ms. Monegato, is an adult individual residing in Geneva, Illinois. Ms. Monegato is a former FCI patient and Data Breach victim, receiving notice in December 2021 that her PHI and PII were compromised.

12. Defendant, FCI, is a fertility care provider headquartered at 2555 Patriot Blvd., Glenview, Illinois 60026.

JURISDICITON & VENUE

13. This Court has subject-matter jurisdiction over this class action lawsuit because it arises under Illinois law.

14. This Court has personal jurisdiction over FCI under 735 ILCS5/2-209 because Ms. Monegato's claims arise out of and relate to FCI's conduct in Illinois.

15. Venue is proper in this Court under 735 ILCS 5/2-101(2) because the transactions or some part thereof out of which the cause of action arouse occurred in Cook County.

FACTUAL BACKGROUND

FCI

16. FCI is a for-profit fertility clinic system headquartered in northern Illinois, with nine locations around the state.

17. FCI's clinic system offers services and care to patients seeking fertility treatment and preservation, including diagnostic and surgical procedures, intrauterine insemination, in vitro fertilization, egg freezing, and embryo cryopreservation.

18. FCI understands the sensitive nature of the services it provides, marketing that it knows its patients may be "anxious" over the "uncertainty of the outcome of infertility treatment [and] the basic lack of control over the process[.]" FCI markets that it assists patients through this "Emotional Journey" in seeking its treatment.

19. As part of its services, FCI requires that its patients disclose their PHI and PII, including their names, Social Security numbers, financial account information, payment card information, treatment information, diagnosis, treating/referring physicians, medical record number, medical billing/claims information, and prescription/medication information.

20. In exchange for this information, FCI promises to safeguard its patients' PHI and PII, providing them privacy policies.

21. FCI's Notice of Privacy Practices ("Privacy Notice") recognizes FCI's duty to securely maintain its patients' PHI and PII: "We understand that your medical information is private and confidential. Further, we are required by law to maintain the privacy of 'Protected Health Information (PHI).' Protected health information includes any individually identifiable information that we obtain from you or others that relates to your past, present or future physical or mental health, the health care you have received or payment for your health care."

22. Indeed, the Privacy Notice lists FCI's "responsibilities" in protecting patient data. Notably, the Privacy Notice states that FCI is "required" to: (i) Maintain the privacy of patients'

PHI; (ii) provide patients notice about its privacy practices; and (iii) "Where required by law, notify you in the event that there has been a breach of your unsecured health information[.]"[2]

Our Responsibilities

We are required to:

- Maintain the privacy of your health information
- Provide you with a notice as to our legal duties and privacy practices with respect to information we collect and maintain about you
- Abide by the terms of this notice
- Notify you if we are unable to agree to a requested restriction
- Accommodate reasonable requests you may have to communicate health information by alternative means or at alternative locations
- Where required by law, notify you in the event that there has been a breach of your unsecured health information
- We reserve the right to change our practices and to make the new provisions effective for all Protected Health Information we maintain.
- Should our information practices change, we will post the revised Notice of Privacy Practices on our website at fcionline.com, as well as at our offices, and provide you with a hard copy upon request.

FCI Fails to Safeguard Patients' PHI and PII

23. Ms. Monegato and the proposed Class are current and former FCI patients.

24. As a condition to providing treatment, FCI required Ms. Monegato and the proposed Class to provide their PHI and PII.

25. FCI then collected and maintained their PHI and PII in its computer systems.

26. On information and belief, FCI stored patient PHI and PII in multiple locations, all using different security safeguards.

[2] https://www.fcionline.com/notice-of-privacy-practices (last visited Jan. 24, 2022).

27. On information and belief, although FCI stores some PHI and PII in what it considers to be a dedicated electronic medical records, or "EMR," system, it nevertheless stores electronic medical records in different systems with less secure safeguards.

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

29. On information and belief, FCI is aware that cybercriminals attacked one of its vendors, US Fertility, in a September 2020 breach that implicated FCI information.

30. Sometime on or before February 1, 2021, cybercriminals infiltrated FCI's systems and accessed patient PHI and PII.

31. On information and belief, cybercriminals were able to do so using and FCI administrative account, giving them high-level access to FCI's systems and patient PHI and PII.

32. On information and belief, FCI did not have adequate security protocols to prevent, detect, and stop the hackers from accessing troves of PHI and PII.

33. On February 1, 2021, FCI learned of the Data Breach by detecting "suspicious activity" on its systems. According to the Breach Notice, FCI purportedly "took immediate steps to conduct a thorough and comprehensive review of its records to identify the files accessed, the information contained in those files, and to whom that information pertained."

34. FCI was initially unable to determine the Data Breach's scale and knew only that hackers "had gained access to a number of FCI's administrative files, and folders containing certain data."

35. Despite FCI's "immediate" action, it did not immediately inform patients about the Data Breach. Instead, FCI continued its "investigation" for six months, inexplicably dragging it

out while its patients were unaware that cybercriminals had accessed their highly sensitive PHI and PII, including fertility records and payment information.

36. In August 2021, following its six-month investigation, FCI learned that hackers had, in fact, accessed a vast trove of PHI and PII.

37. Though it had taken FCI six months to "investigate" this disturbing Data Breach, FCI *still* did not immediately inform its patients and regulators about the breach, choosing instead to wait another four months.

38. In December 2021, FCI finally admitted to the breach to the U.S. Department of Health and Human Services ("DHHS"). DHHS is currently investigating the Data Breach.

39. In its Breach Notice[3] to patients, FCI obfuscated the true nature of the the Data Breach, indicating in bold-faced and underlined type that cybercriminals had not access patients' medical records:

> **On February 1, 2021, FCI became aware of suspicious activity on its internal systems. In response, FCI engaged independent forensic investigators to conduct an investigation of the activity. The investigation revealed that an unauthorized third party had gained access to a number of FCI's administrative files, and folders containing certain data. Due to the security systems already in place, the investigation indicated that no EMR (electronic medical records) systems were accessed or otherwise compromised as a result of this incident. FCI took immediate steps to conduct a thorough and comprehensive review of its records to identify the files accessed, the information contained in those files, and to whom that information pertained. On August 27, 2021, FCI determined that information related to certain FCI patients was included in the set of files accessed by the unauthorized third party. FCI is not aware of any actual or attempted misuse of patient information as a result of this incident.**

40. This disclosure is inaccurate, as the Breach Notice's next paragraph makes clear that hackers had accessed several types of patient information, including patients' electronic medical records:

[3] A true and correct copy of the Breach Notice is attached as **Exhibit A.**

The impacted files contained personal information including the names of some patients, employer-assigned identification numbers, passport numbers, Social Security numbers, financial account information, payment card information, treatment information, diagnosis, treating/referring physicians, medical record number, medical billing/claims information, prescription/medication information, Medicare/Medicaid identification information, health insurance group numbers, health insurance subscriber numbers, patient account numbers, encounter numbers, ill health / retirement information, master patient index, occupational-health related information, other medical benefits and entitlements information, other medical identification numbers, patkeys/reason for absence, sickness certificate, usernames and passwords with PINs or account login information, and medical facilities associated with patient information.

41. The Breach Notice did not explain who breached FCI's systems, how the Data Breach occurred, how FCI learned about the breach, or why FCI took over *10 months* to notify patients that their highly sensitive PHI and PII had been accessed by cybercriminals.

42. The Breach Notice then explained what FCI was doing to prevent future breaches, including implementing enterprise identity verification software and employee training—all of which should have been in place before the Data Breach.

43. As a result of FCI's Data Breach, its victims face a lifetime risk of identity theft, as it includes sensitive information that cannot be changed, like their dates of birth and Social Security numbers. Despite this lifetime risk, FCI offered its victims only 12 to 24 months of identity theft protection services.

44. On information and belief, FCI failed to adequately train its employees on reasonable cybersecurity protocols or implement reasonable security measures, causing it to lose control over patients' PII and PHI. FCI's negligence is evidenced by its failure to recognize the Data Breach until cybercriminals had already accessed patient data, meaning FCI had no effective means to detect and prevent attempted data breaches. Further, the Breach Notice makes clear that FCI is unwilling and unable to communicate the scope of the Data Breach, misrepresenting that no "EMR" was compromised while also disclosing that cybercriminals access electronically stored medical records. FCI should have had adequate security protocols in place before the Data Breach, especially considering that FCI was on-notice of a similar breach involving its vendor, US Fertility.

Plaintiff's Experience

45. Ms. Monegato is a former FCI patient.

46. As a condition of receiving FCI's services, FCI required Ms. Monegato to provide her PHI and PII.

47. Ms. Monegato provided her PHI and PII as part of receiving FCI's services.

48. Ms. Monegato received FCI's Breach Notice and became aware that her PHI and PII were compromised in the Data Breach.

49. Ms. Monegato was disturbed by the Data Breach's nature and the thought of cybercriminals accessing her highly sensitive PHI and PII. She was also outraged that FCI had taken over 10 months to tell her about the Data Breach, without explaining its delay or why it refused to disclose the breach months after it *knew* her information had been compromised.

50. Ms. Monegato has spent considerable time and effort monitoring her accounts to protect herself from additional identity theft. Ms. Monegato fears for her personal financial security and uncertainty over what medical information was revealed in the Data Breach. She is experiencing feelings of anxiety, sleep disruption, stress, and fear because of the Data Breach. This goes far beyond allegations of mere worry or inconvenience; it is exactly the sort of injury and harm to a Data Breach victim that is contemplated and addressed by law.

51. Further, Ms. Monegato is unsure what has happened to her PII and PHI as FCI has been unwilling to disclose the true nature of the Data Breach.

Ms. Monegato and the Proposed Class Face Significant Risk of Identity Theft

52. Ms. Monegato and members of the proposed Class have suffered injury from the misuse of their PII and PHI that can be directly traced to FCI.

53. The ramifications of FCI'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.

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

55. Because FCI failed to prevent the Data Breach, Ms. Monegato and the proposed Class have suffered and will continue to suffer damages, including monetary losses, lost time, anxiety, and emotional distress. They have suffered or are at an increased risk of suffering:

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

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

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

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

60. 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;

61. Delay in receipt of tax refund monies;

62. Unauthorized use of stolen PII and PHI; and

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

64. 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.

65. 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, like Marketo, making the information publicly available, for a fee.

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

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

68. Cybercriminals can cross-reference two 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.

69. 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.

70. 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.

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

72. 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.

73. Along with out-of-pocket expenses that can exceed thousands of dollars for the victim of new account identity theft, and the emotional toll identity theft can take, some victims must spend a considerable time repairing the damage caused by the theft of their 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.

74. 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, Ms. Monegato and the Class will need to remain vigilant against unauthorized data use for years or even decades to come.

75. 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."

76. 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.

77. 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.

78. 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

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

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

All individuals residing in Illinois whose PHI and PII was compromised in the Data Breach disclosed by FCI in December 2021.

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

82. The Class defined above is identifiable through FCI's business records.

83. There are nearly 80,000 potential Class members.

84. Individual joinder of these persons is impracticable.

85. Plaintiff is a member of the Class.

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

a. Whether FCI had a duty to use reasonable care in safeguarding Ms. Monegato and the Class's PII and PHI;

b. Whether FCI 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 FCI was negligent in maintaining, protecting, and securing PII and PHI;

d. Whether FCI breached contract promises to safeguard Ms. Monegato and the Class's PII and PHI;

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

f. Whether FCI's Breach Notice was reasonable;

g. Whether the Data Breach caused Ms. Monegato and the Class injuries;

h. What the proper damages measure is;

i. Whether FCI violated the statutes alleged in this complaint; and

j. Whether Ms. Monegato and the Class are entitled to damages, treble damages, or injunctive relief

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

88. 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.

89. 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. The only individual question concerns identification of Class members, which will be ascertainable from records maintained by FCI.

90. 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.

91. 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)

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

93. 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.

94. 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 providing access to this information to 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.

95. 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.

96. 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. Plaintiff and members of the Class needed to provide their PII and PHI to Defendant to receive medical treatment and services from Defendant, and Defendant retained that information.

97. 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.

98. 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.

99. 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 and 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. 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. 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 monetary damages, increased risk of future harm, embarrassment, humiliation, frustration, and emotional distress.

100. 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.

SECOND CLAIM FOR RELIEF
Negligence Per Se
(On Behalf of Plaintiff and the Class)

101. Plaintiff and members of the Class incorporate the above allegations as if fully set forth herein.

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

103. 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' PII. 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.

104. Defendant violated its duty under Section 5 of the FTC Act by failing to use reasonable measures to protect its patients' PII 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 Defendant had collected and stored and the foreseeable consequences of a data breach, including, specifically, the immense damages that would result to its patients in the event of a breach, which ultimately came to pass.

105. 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.

106. 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.

107. 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.

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

109. 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.

110. 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.

111. Had Plaintiff and members of the Class known that Defendant did not adequately protect patients' PII, Plaintiff and members of the Class would not have entrusted Defendant with their PII.

112. As a direct and proximate result of Defendant's negligence per se, Plaintiff 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 received had they known of Defendant's careless approach to cyber security; lost control over the value of PII; 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.

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

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

114. A valid and enforceable contract existed between FCI and Plaintiff and the Class.

115. FCI's Privacy Notice states the terms of FCI's performance in securely maintaining Plaintiff and the Class's PHI and PII. The Privacy Notice states that FCI is required to "abide by the terms of this [Privacy Notice]," including that FCI (i) Maintain the privacy of patients' PHI; (ii) provide patients notice about its privacy practices; and (iii) "Where required by law, notify [patients] in the event that there has been a breach of [patients'] unsecured health information[.]"

116. These terms are valid and enforceable against FCI.

117. Plaintiff and the Class substantially performed under the terms of the Privacy Notice.

118. FCI breached the terms of the Privacy Notice and its contract with Plaintiff and the Class by failing to: (i) maintain the privacy of Plaintiff and the Class's PII and PHI; and (ii) timely notify Plaintiff and the Class about the breach of their unsecured information consistent with Illinois state law.

119. FCI's breaches have injured Plaintiff and the Class, proximately causing them substantial injuries, entitling them to damages, restitution, and other relief in an amount to be proven at trial.

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

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

121. Plaintiff alleges this claim in the alternative to their express breach of contract claim.

122. Defendant offered to provide goods and services to Plaintiff and members of the Class in exchange for payment.

123. Defendant also required Plaintiff and the members of the Class to provide Defendant with their PII and PHI to receive services.

124. In turn, and through the Notice of Privacy Practices, Defendant agreed it would not disclose the PHI it collects from patients to unauthorized persons. Defendant also impliedly promised to maintain safeguards to protect its patients' PII and PHI.

125. Plaintiff and the members of the Class 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.

126. 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.

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

128. Defendant materially breached the contract(s) 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:

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

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

131. Failing to ensure the confidentiality and integrity of electronic PII and PHI that Defendant created, received, maintained, and transmitted in violation of 45 C.F.R. § 164.306(a)(1).

132. 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 agreement(s).

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

134. The convent 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.

135. 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.

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

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

138. 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.

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

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

140. This claim is plead in the alternative to the breach of contract and implied contractual duty claims.

141. Plaintiff and members of the Class conferred a monetary benefit upon Defendant in the form of monies paid for treatment services.

142. 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 PHI, as this was used to facilitate payment and treatment services.

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

144. Under principals of equity and good conscience, Defendant should not be permitted to retain the money belonging to Plaintiff and members of the Class because Defendant failed to implement (or adequately implement) the data privacy and security practices and procedures for itself that Plaintiff and members of the Class paid for and that were otherwise mandated by federal, state, and local laws and industry standards.

145. 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.

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

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

147. 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.

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

149. 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 Ill. Comp. Stat. 530/45(a).

150. The IPIPA further requires that data collectors 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. 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).

151. 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.

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

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 Ms. Monegato and the proposed Class, appointing Ms. Monegato 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 Ms. Monegato and the Class;

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

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

E. Awarding Ms. Monegato 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. Awarding prejudgment and post-judgment interest, as provided by law;

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

J. 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.

RESPECTFULLY SUBMITTED AND DATED this 31st day of January, 2022.

Respectfully submitted,

/s/ J. Gerard Stranch
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
peterj@bsjfirm.com

/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