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

| | | |
|---|---|---|
| JANE DOE, individually and as the representative of a class of similarly situated persons,<br><br>Plaintiff,<br><br>v.<br><br>US FERTILITY, LLC, a Delaware limited liability company, and FERTILITY CENTERS OF ILLINOIS, S.C., an Illinois corporation,<br><br>Defendants. | ) | Case No.: 1:21-CV-00579 |

**FIRST AMENDED CLASS ACTION COMPLAINT**

Plaintiff, JANE DOE ("Plaintiff"), through her attorneys, brings this action on behalf of herself and all others similarly situated and alleges the following against Defendants, US FERTILITY, LLC ("USF") and FERTILITY CENTERS OF ILLINOIS, S.C. ("Fertility Centers") (collectively "Defendants"):

**PRELIMINARY STATEMENT**

1. Plaintiff brings this class action lawsuit against Defendants for their failure to protect their patients' personal information – including protected health information as defined by the Health Insurance Portability and Accountability Act ("HIPAA") Pub.L. 104-191, 110 Stat. 1936, Aug. 21, 1996, Social Security numbers, and dates of birth (collectively, "Personal Information") – as statutorily and contractually required.

2. Defendants, as medical practitioners and fertility specialists, are required to protect their patients' Personal Information by adopting and implementing the specific data and security regulations and standards set forth pursuant to HIPAA.

3. According to guidelines published by the Federal Trade Commission ("FTC"), Defendants must also: (a) protect customers' personal information – including encrypting information stored on computer networks and implementing policies to address security issues; (b) properly dispose of customer information when it is no longer needed: and (c) understand vulnerabilities on their network. Businesses also should have systems in place to detect intrusions and expose breaches as soon as they occur.

4. Finally, Defendants expressly promised to safeguard their patients' Personal Information in accordance with HIPAA regulations and industry standards through their privacy policies and patient agreements. Without such policies and agreements, patients, including Plaintiff, would not have entrusted Defendants with their care.

5. Notwithstanding their statutory and contractual obligations, Defendants failed to protect their patients' Personal Information. On January 8, 2021, USF sent Plaintiff a letter detailing an "IT security event" ("Data Breach") that occurred on September 14, 2020. A copy of that letter is attached as Exhibit A.

6. According to Defendants, an "unauthorized actor" gained access to an unknown number of their patient files, including Plaintiff's files. These compromised files contained patient names, Social Security numbers, dates of birth, and patient file numbers. The "unauthorized actor" had access to the files for over a month.

7. Although aware of the Data Breach, Defendants waited almost four months to inform Plaintiff that her Personal Information was compromised, and/or stolen.

8. As a result of Defendants' misconduct, Personal Information of Plaintiff and other impacted patients were compromised and made available to criminals for misuse. The injuries that Plaintiff and these other patients have and will continue to suffer include:

a) theft of personal information;

b) costs associated with the detection and prevention of identity theft;

c) costs associated with spending time to address and mitigate the actual and future consequences of Defendants' failure to safeguard Personal Information, such as time taken from the enjoyment of one's life and the inconvenience, nuisance, cost, and annoyance of dealing with all the issues resulting from the exposure of their Personal Information;

d) the imminent and impending injury resulting from the potential fraud and identity theft posed by the Personal Information being exposed for theft and sale;

e) damages to and diminution in value of the Personal Information that Defendants were entrusted to keep secure; and

f) the invasion of privacy, which is particularly troubling here since the Personal Information relates to the most sensitive of information – the attempt to have a child.

9. Defendants directly and proximately caused the injuries Plaintiff and other impacted patients suffered by failing to implement or maintain adequate data security measures for Personal Information, failing to timely respond to the breach of the Personal Information, and failing to promptly notify impacted patients of the exposure of their Personal Information.

10. Defendants have acknowledged the injuries and impending injuries caused by their failures to safeguard Personal Information by offering temporary monitoring services to all impacted patients. (*See* Ex. A). However, these services do not and cannot prevent or rectify the full extent of injuries suffered by Plaintiff and the other impacted patients and will suffer far into the future.

11. Plaintiff and other impacted patients retain a significant interest in ensuring that their Personal Information, which remains in Defendants' possession, is protected from further

exposure.

12. Thus Plaintiff, on behalf of herself and all others similarly situated, brings this case as a class action asserting claims against Defendants for breach of contract, breach of implied contract, unjust enrichment, breach of fiduciary duty, invasion of privacy, and violations of the Illinois Consumer Fraud and Deceptive Business Practices Act. 815 ILCS § 505/2, *et seq.* ("ICFA" or "Act").

13. This action is based upon a common nucleus of operative facts because Defendants failed to protect the Personal Information of Plaintiff and other impacted patients in an identically insufficient manner. This action is based on the same legal theory, namely, liability for Defendants' failure to institute adequate security measures to protect their patients' Personal Information and promptly inform Plaintiff and other impacted patients as quickly as possible after the Data Breach occurred.

14. This action seeks to recover damages, and obtain equitable relief, including injunctive relief designed to prevent a reoccurrence of a data breach and resulting injuries, restitution, disgorgement, reasonable costs and attorneys' fees, and any other remedies this Court deems proper.

## PARTIES

15. Plaintiff is, and was at all times relevant to this matter, a citizen of the State of Illinois and resident of DuPage County, Illinois. Plaintiff is a former patient of Fertility Centers.

16. USF is the largest physician-owned, physician-led partnership of top-tier IVF/fertility practices in the United States.[1] USF is incorporated in Delaware, with its principal place of business located in Rockville, Maryland.

[1] Information obtained from USF's website, www.usfertility.com, last visited on February 1, 2021.

17. On information and belief, USF was formed through a partnership with numerous fertility centers throughout the United States, including Fertility Centers, and Amulet Capital Partners, a private equity firm. USF's network is comprised of 55 locations across ten states. Through its clinics and more than 80 physicians, USF completed nearly 25,000 in vitro fertilization cycles in 2018.

18. Fertility Centers is a service corporation that operates fertility centers throughout Illinois. Fertility Centers is part of the USF partnership.

## JURISDICTION AND VENUE

19. The United States District Court for the Northern District of Illinois, Eastern Division, has jurisdiction over this matter pursuant to 28 U.S.C. § 1332(d)(2) (the "Class Action Fairness Act") because sufficient diversity of citizenship exists between the parties – Plaintiff is a citizen of Illinois and USF is incorporated in Delaware, with its principal place of business located in Rockville, Maryland. Further, the aggregate amount in controversy exceeds $5,000,000, exclusive of interest and costs, with at least 100 or more potential class members based on published news reports of the impacts of Defendants' Data Breach and the size and scope of Defendants' practice. The Court has supplemental jurisdiction over the state law claims pursuant to 28 U.S.C. § 1367.

20. The Court has personal jurisdiction over Defendants because they are authorized to do business in this District and regularly conduct business in this District and, with respect to Fertility Centers, maintains its principal place of business within this District.

21. Venue is proper in this District pursuant to 28 U.S.C. § 1391(b)(2) in that a substantial part of the events or omissions giving rise to Plaintiff's claims occurred in this District.

## FACTUAL ALLEGATIONS

### The devastating impact of data breaches and the importance of protecting personal information.

22. The healthcare industry is among the worst affected by data breaches. From 2005 to 2019, the total number of individuals affected by healthcare data breaches was 249.09 million, of which 157.40 million were affected in the last five years alone.[2] According to the 2020 HIMSS Cybersecurity Survey, significant cybersecurity incidents are now the norm with "threat actors" seeking financial information, employee information, and patient information.[3]

23. Personally identifiable information is a valuable commodity to identity thieves. As recognized by the FTC, with the Personal Information at issue here, identity thieves can commit an array of crimes including identity theft and medical and financial fraud.[4] In fact, the Personal Information here is particularly valuable because criminals can use it to target victims with frauds and scams that take advantage of the victim's medical condition. It also can be used to create fake insurance claims, allowing for the purchase and resale of medical equipment, and to gain access to prescriptions for illegal use or resale, or lead to data tampering, which can result in faulty treatment, with fatal and irreversible losses to patients.[5] Finally, it can be used to embarrass or blackmail the impacted patients.

---

[2] *Healthcare Data Breaches: Insights and Implications*, US National Library of Medicine, Healthcare (Basel). 2020 Jun; 8(2): 133.

[3] https://www.himss.org/sites/hde/files/media/file/2020/11/16/2020_himss_cybersecurity_survey_final.pdf (last visited on February 1, 2021).

[4] Federal Trade Commission, *Warning Signs of Identity Theft, https://www.consumer.ftc.gov/articles/0271-warning-signs-identity-theft* (last visited on February 1, 2021).

[5] *Healthcare Data Breaches: Insights and Implications*.

24. The ramifications of a failure to safeguard Personal Information are long lasting and severe. The risks of fraud and identity theft to those whose Personal Information has been compromised can last a lifetime.[6]

**Guidelines under HIPAA, FTC, and state law establish standards for safeguarding personal information.**

25. Due to the important nature of ensuring the security of personally identifiable information, the federal government has issued guidelines for safeguarding such information under both HIPAA and the FTC. In fact, one of the purposes of HIPAA is to establish national privacy standards regarding individually identifiable health information. *Law v. Zuckerman*, 307 F. Supp. 2d 705, 710 (D. Md. 2004).

26. Title II of HIPAA contains what are known as the Administrative Simplification provisions. 42 U.S.C. §§ 1301, *et seq.* These provisions require, among other things, that the Department of Health and Human Services ("HHS") create rules to streamline the standards for handling personally identifiable information and protected health information, like the information Defendants failed to safeguard here.

27. Pursuant to its mandate, HHS established that entities in possession of personally identifiable information and protected health information must:

a. ensure the confidentiality, integrity, and availability of all electronic protected health information the entity creates, receives, maintains, or transmits (45 C.F.R. § 164.306(a)(1));

b. protect against any reasonably anticipated threats or hazards to the security or integrity of such information (45 C.F.R. § 164.306(a)(2));

[6] *https://www.aarp.org/money/scams-fraud/info-2019/medical-records-identity-theft/* (last visited on February 1, 2021).

c. protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required (45 C.F.R. § 164.306(a)(3));

d. implement policies and procedures to prevent, detect, contain, and correct security violations (45 C.F.R. § 164.308(1));

e. implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights (45 C.F.R. § 164.312(a)(1));

f. have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information (45 C.F.R. § 164.530(c)(1)); and

g. mitigate, to the extent practicable, any harmful effect that is known of a use or disclosure of protected health information (45 C.F.R. § 164.530(f)).

28. The FTC guidelines establish fundamental data security principles and practices for businesses. According to the FTC, the need for data security should be factored into all business decision-making.[7]

29. The FTC guidelines can be found in its publication entitled *Protecting Personal Information: A Guide for Business*.[8] The guidelines note businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand vulnerabilities of its network; and implement policies to correct security problems.[9] The guidelines also recommend

[7] Federal Trade Commission, *Start With Security*, available at *https://www.ftc.gov/tips-advice/business-center/guidance/start-security-guide-business#start* (last visited on February 1, 2021).

[8] Federal Trade Commission, *Protecting Personal Information: A Guide for Business*, available at *https://www.ftc.gov/tips-advice/business-center/guidance/protecting-personal-information-guide-business* (last visited on February 1, 2021).

[9] *Id.*

that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[10]

30. Pursuant to Section 5 of the FTC Act (15 U.S.C. § 45), failure to protect Personal Information can constitute an unfair act or practice.

31. The state of Illinois has also addressed the protection of Personal Information by enacting the Personal Information Protection Act ("PIPA"), 815 ILCS 530/1 *et seq.* PIPA requires any entity that maintains or stores Personal Information to "notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person." 815 ILCS 530/10 (a) and (b).

32. Failure to comply with PIPA constitutes an unlawful practice under ICFA. 815 ILCS § 530/20.

**Defendants' Privacy Policies and the Data Breach.**

33. As a condition of using their services, Defendants required Plaintiff to provide personal identifying information prior to becoming a patient, including, among other things, the individual's medical records, insurance card, identification card, date of birth, and Social Security number. On information and belief, Defendants require all individuals seeking to use their services to provide the personal identifying information listed above prior to becoming a patient.

[10] *Id.*

34. According to USF, "[a]s a Business Associate of the Network Practices,[11] which are Covered Entities under [HIPAA] and its implementing regulations … [USF] maintains protected health information in compliance with HIPAA and our contractual obligations to the Network Practices." [12]

35. In its Notice of Privacy Practices, Fertility Centers indicates that a patient's health records "is the physical property of Fertility Centers."[13]

36. According to Fertility Centers, it is required to: "maintain the privacy of your health information … abide by the terms of this notice … [and] where required by law, notify you in the event that there has been a breach of your unsecured health information." [14]

37. Moreover, by obtaining, collecting, using, and deriving a benefit from the Personal Information of Plaintiff and other impacted patients, Defendants assumed legal and equitable duties to those individuals.

38. Notwithstanding these policies and assurances, Defendants failed to properly safeguard Plaintiff's and impacted patients' Personal Information. As stated, on September 14, 2020, Defendant experienced a Data Breach which involved the inaccessibility of certain computer systems on Defendants' network as a result of a malware infection.

39. According to Defendants, data on a number of servers and workstations connected to their domain had been encrypted by ransomware. During the Data Breach, an unauthorized actor acquired files throughout the period of unauthorized access, which extended from August 12, 2020

[11] "Network Practices" is in reference to the fertility centers that partnered together to form USF.

[12] Information from USF's website, www.usfertility.com, last visited on February 1, 2021.

[13] Information from Fertility Centers' website, www.fcionline.com, last visited on February 1, 2021.

[14] *Id.*

to September 14, 2020.

40. After a review of the Data Breach by a retained third-party computer forensic specialist, it was determined that impacted patients, including Plaintiff, had their names, Social Security numbers, Patient Number/MPI, and dates of birth revealed to the unauthorized actor.

41. Although Defendants became aware of the Data Breach on September 14, 2020, they did not contact Plaintiff until January 8, 2021 – almost four months after the occurrence.

42. In an apparent attempt to mitigate the damage caused by the Data Breach, Defendants offered to provide Plaintiff with twelve months of complimentary access to credit monitoring and identity restoration services.

43. Defendants were aware of their obligations to protect the Personal Information of Plaintiff and other impacted patients as made clear in their privacy notices. At all relevant times, Plaintiff and the impacted patients had taken all reasonable steps to maintain the confidentiality of their Personal Information and were assured that Defendants would do the same.

44. Defendants were aware of the guidelines set forth under HIPAA, the FTC, and PIPA regarding protecting their patients' Personal Information.

45. On information and belief, Defendants inability to safeguard Plaintiff's Personal Information is, in part, a result of their:

a. failing to ensure the confidentiality, integrity, and availability of all electronic protected health information the entity creates, receives, maintains, or transmits;

b. failing to protect against any reasonably anticipated threats or hazards to the security or integrity of such information;

c. failing to protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required;

d. failing to implement policies and procedures to prevent, detect, contain, and correct security violations;

e. failing to implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights;

f. failing to have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information;

g. failing to mitigate, to the extent practicable, any harmful effect that is known of a use or disclosure of protected health information and to notify Plaintiff and the impacted patients immediately after the Data Breach occurred; and

h. failing to properly dispose of customer information when it was no longer required to be held – Defendants retained some impacted patient information for up to fourteen years after the doctor/patient relationship ceased with no embryos, eggs, or sperm in storage.

46. On information and belief, Defendants had the resources necessary to prevent the Data Breach but neglected to adequately invest in data security measures despite their obligation to protect Personal Information.

47. Had Defendants remedied the deficiencies in their data security systems and adopted security measures recommended by experts in the field, they would have prevented the intrusion into their system and, ultimately, the theft of the Personal Information of Plaintiff and other impacted patients.

**Plaintiff's Experience.**

48. On or about October 24, 2011, Plaintiff visited Fertility Centers' Hinsdale, Illinois location in the hopes of having a child.

49. During her initial consultation, Defendants requested that Plaintiff provide them with proof of insurance, an identification card, medical records, and her Social Security number. Defendants also asked Plaintiff to describe any medical issues she may have on an intake form. In order to proceed with the consultation, Plaintiff complied.

50. Plaintiff paid Defendants for her consultation. Part of this payment was for the protection of her Personal Information. But for this protection, Plaintiff would not have shared her Personal Information nor sought treatment from Defendants.

51. After her initial consultations, Plaintiff elected to not become a patient of Defendants and received no treatments from them.

52. Plaintiff's visit to Fertility Center's location was over eleven years ago. There is no reason for Defendants to have retained Plaintiff's Personal Information for so long, especially since Plaintiff elected to forego treatment with Defendants.

53. Since Plaintiff only consulted with Defendants, and that consultation was over eleven years ago, she was shocked to learn that her Personal Information was exposed during the Data Breach. Defendants' Notice of the Data Breach not only caused Plaintiff tremendous anxiety, it also required her to complete a credit check with her bank and to freeze her credit with the various credit monitoring agencies.

54. In addition, Plaintiff will have to endure the risks of identity theft and fraud for years to come. She will also have to live with the idea that her private medical affairs are now in the possession of cybercriminals, with the potential to be publicized and forever available to the public. All this from a consultation that occurred over eleven years ago and went nowhere.

55. Thus, as a direct and proximate result of Defendants' failure to safeguard Personal Information, Plaintiff and other impacted patients have been placed in an imminent, immediate,

and continuing increased risk of harm from identity theft and fraud, requiring them to take the time, which they otherwise would have dedicated to other life demands such as work and family, in an effort to mitigate the actual and potential impact of the Data Breach.

56. In sum, as a result of Defendants' failures to prevent the Data Breach and their inadequate response to it afterwards, Plaintiff and other impacted patients have suffered, will suffer, or are at increased risk of suffering:

a. the compromise, publication, theft, and/or unauthorized use of their Personal Information;

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 Personal Information, which remains in the possession of Defendants and is subject to further breaches so long as Defendants fail to undertake appropriate measures to protect Personal Information in their possession;

e. emotional distress and embarrassment over the publication of the reproductive medical issues, care, and treatments of Plaintiff and the impacted patients.

f. 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 impacted patients.

57. Plaintiff and the other impacted patients maintain an undeniable interest in ensuring that their Personal Information is secure, remains secure, and is not subject to further misappropriation and theft.

## CLASS ACTION ALLEGATIONS

58. Pursuant to Federal Rule of Civil Procedure 23(a) and (b)(3), Plaintiff brings this class action on behalf of herself and the following National Class and Illinois Subclass (collectively "the Class"):

**A. National Class:**

> All persons residing in the United States who were patients of USF and/or Fertility Centers and whose Personal Information was accessed without authorization as a result of the Data Breach.

**B. Illinois Subclass for Violation of Illinois Consumer Fraud Act:**

> All persons residing in the State of Illinois who were patients of USF and/or Fertility Centers and whose Personal Information was accessed without authorization as a result of the Data Breach.

Excluded from the Class are Defendants and its employees and agents and members of the Judiciary. Plaintiff reserves the right to amend the Class definitions upon completion of class discovery when the contours and the parameters of class become more apparent.

59. Class Size (Fed. R. Civ. P. 23(a)(1)): On information and belief, the Class consists of more than forty (40) and likely thousands of persons who are identifiable through Defendants' records, and is so numerous that joinder of all members is impracticable.

60. Commonality (Fed. R. Civ. P. 23 (a)(2)): There are questions of fact or law common to the class predominating over all questions affecting only individual Class Members including:

a. Whether Defendants engaged in wrongful conduct as alleged herein;

b. Whether Defendants owed a duty to Plaintiff and the Class to adequately protect their Personal Information and to provide timely and accurate notice of the Data Breach to Plaintiff and the Class Members and whether Defendants breached these duties;

c. Whether Defendants willfully, recklessly, or negligently failed to maintain and execute reasonable procedures to prevent unauthorized access to their data security networks and to the Personal Information of Plaintiff and the Class;

d. Whether Defendants conduct, or failure to act, resulted in or was the proximate cause of the Data Breach;

e. Whether Defendants' security measures to protect their computer systems were reasonable under FTC data security recommendations and best practices recommended by security experts;

f. Whether Defendants failed to protect Plaintiff and the Class by allowing unauthorized access to their Personal Information;

g. Whether Defendants continue to breach the duties they owe to Plaintiff and the Class;

h. Whether Defendants actions as described herein are unfair and oppressive and thus, in violation of ICFA; and

i. Whether Plaintiff and the Class are entitled to actual damages and equitable relief as a result of the Data Breach.

61. Typicality (Fed. R. Civ. P. 23(a)(3)): Plaintiff's claims are typical of the claims of all Class Members and Plaintiff and the Class have suffered similar injuries as a result of Defendants' practices alleged herein.

62. Fair and Adequate Representation (Fed. R. Civ. P. 23(a)(4)): Plaintiff will fairly and adequately protect the interests of the other Class Members. Plaintiff has retained counsel who are experienced in handling class actions and claims involving unlawful business practices. Neither Plaintiff nor her counsel have any interests adverse or in conflict with the Class.

63. Predominance and Superiority (Fed. R. Civ. P. 23(b)(3)): Common questions of law and fact predominate over any questions affecting only individual members, and a class action is superior to other methods for the fair and efficient adjudication of the controversy because:

(a) Proof of liability on Plaintiff's claims will also prove liability for the claims of the Class without the need for separate or individualized proceedings;

(b) Evidence regarding defenses or any exceptions to liability that Defendants may assert and attempt to prove will come from Defendants' records and will not require individualized or separate inquiries or proceedings;

(c) Defendants have acted and are continuing to act pursuant to common policies or practices in the same or similar manner with respect to all Class Members;

(d) The injury suffered by each Class Member, while meaningful on an individual basis, is not of such magnitude as to make the prosecution of individual actions against Defendants economically feasible. Even if Class Members could afford individual litigation, those actions would put immeasurable strain on the court system. A class action, on the other hand, will permit a large number of claims involving virtually identical facts and legal issues to be resolved efficiently in one proceeding based upon common proofs; and

(e) This case is inherently manageable as a class action in that:

(i) Defendants' records and court filings will enable Plaintiff to readily identify class members and establish liability and damages;

(ii) Liability and damages can be established for Defendants and the Class with the same common proofs;

(iii) A class action will result in an orderly and expeditious administration of claims and it will foster economics of time, effort, and expense;

(iv) A class action will contribute to uniformity of decisions concerning Defendants' practices; and

(v) As a practical matter, the claims of the Class are likely to go unaddressed absent class certification.

**COUNT I**

**BREACH OF CONTRACT**

64. Plaintiff incorporates paragraphs 1 through 57 as if fully stated herein.

65. Plaintiff and the Class entered into valid and enforceable agreements, which are in the custody and control of Defendants, whereby Defendants promised to provide health care to Plaintiff and the Class, and Plaintiff and the Class agreed to pay money for such services**.**

66. A material part of Defendants' promise to provide health care services to Plaintiff and the Class was to adequately protect their Personal Information.

67. In their privacy policies, Defendants expressly promised Plaintiff and the Class that they would comply with all HIPAA standards, maintain the privacy of their Personal Information, and only disclose their health information when required by law.

68. The contracts required Defendants to safeguard Plaintiff's and Class Members' Personal Information and prevent disclosure and/or unauthorized access of such information through its data security measures and prompt disposal of Personal Information that is no longer

needed or required. In the event of an unauthorized disclosure, Defendants were also required to provide timely notice to Plaintiff and the Class.

69. A meeting of the minds occurred, as Plaintiff and Class Members agreed, among other things, to provide correct personal and health information and to pay Defendants for services, which include, protection for their Personal Information. Without such assurances or protection, Plaintiff and the Class would not have entered into their agreements with Defendants.

70. Defendants did not safeguard Plaintiff's and the Class Members' Personal Information. Specifically, Defendants did not fulfill their promise to comply with HIPAA guidelines or industry standards in the manner in which they stored and maintained Personal Information, which resulted in the Data Breach.

71. Defendants also failed to promptly dispose of Personal Information that was no longer needed or required from their network systems, thereby subjecting this information to unnecessary risk.

72. Finally, Defendants failed to provide timely and accurate notice to Plaintiff and the Class that their Personal Information was compromised as a result of the Data Breach, further exposing their Personal Information to additional unnecessary risk of exposure.

73. Defendants' failure to implement sufficient security measures to protect Plaintiff and Class Members' Personal Information as described herein constitutes a breach of an express contract.

74. Defendants' failures to promptly dispose of Personal Information that is no longer needed and provide timely and accurate notice to Plaintiff and the Class that their Personal Information was compromised as a result of the Data Breach as described herein also constitute breaches of an express contract.

75. Defendants' failure to fulfill its data security and management promises resulted in Plaintiff and Class Members receiving services that were of a diminished value (*i.e.,* the provision of medical care without adequate data security and management practices). In other words, because Plaintiff and the Class paid for privacy protections that they did not receive – even though such protections where a material part of their contracts – Plaintiff and the Class did not receive full benefit of their bargain.

76. As a result of Defendants' breaches, Plaintiff and the Class suffered damages in the amount of the difference between the price paid for Defendants' services as promised and the actual diminished value of their health care services and the costs of future monitoring of their credit history for identity theft and fraud.

77. Plaintiff, on behalf of herself and the Class, seeks compensatory damages for breach of an express contract, plus prejudgment interest, and costs.

## COUNT II

### BREACH OF IMPLIED CONTRACT
### (in the alternative to breach of contract)

78. Plaintiff incorporates paragraphs 1 through 57 as if fully stated herein.

79. In order to benefit from Defendants' services, Plaintiff and the Class Members were required to disclose Personal Information to Defendants, including their names, contact information, Social Security numbers, dates of birth, and extremely sensitive medical information.

80. By providing their Personal Information, and upon Defendants' acceptance of such information, Plaintiff and the Class Members on one side, and Defendant, on the other, entered into implied contracts whereby Defendants were obligated to take reasonable steps to secure and safeguard the Personal Information entrusted to them.

81. A meeting of the minds occurred, as Plaintiff and the Class agreed, among other things, to provide their Personal Information and to pay Defendants in exchange for Defendants' agreement to provide medical care and otherwise take reasonable steps to secure and safeguard the Personal Information of Plaintiff and the Class. Such steps necessarily included compliance with all HIPAA and FTC guidelines, prompt disposal of Personal Information that is no longer needed or required, and timely and accurate notification in the event that Plaintiff's and the Class Members' Personal Information became compromised.

82. Without such implied contractual terms, Plaintiff and the Class would not have provided their Personal Information to Defendant.

83. As described herein, Defendants did not take reasonable steps to safeguard Plaintiff's and the Class Members' Personal Information. In short, Defendants' inadequate data security allowed for the Data Breach, their failure to dispose of Personal Information that was no longer needed or required unnecessarily exposed more patients to the Data Breach, and their failure to timely and accurately inform Plaintiff and the Class of the Data Breach recklessly delayed mitigation efforts.

84. Because Defendants allowed unauthorized access to Plaintiff's and the Class Members' Personal Information and failed to take reasonable steps to safeguard their Personal Information, Defendants breached their implied contracts with Plaintiff and the Class.

85. As a result of Defendants' breach, Plaintiff and the Class suffered damages in the amount of the difference between the price paid for Defendants' services as promised and the actual diminished value of their health care services and the costs of future monitoring of their credit history for identity theft and fraud.

86. Plaintiff, on behalf of herself and the other Members of the Class, seeks compensatory damages for breach of implied contract, plus prejudgment interest, and costs.

## COUNT III

### UNJUST ENRICHMENT
### (in the alternative to Counts I and II)

87. Plaintiff incorporates paragraphs 1 through 57 as if fully stated herein.

88. Should the Court find that no contract provision expressly or impliedly governs the claims in Counts I and II, Plaintiff and the Class may be without any adequate remedy at law.

89. Plaintiff and the Class conferred a monetary benefit on Defendants in the form of fees paid for health care services. Part of these services required Defendants to safeguard the Personal Information entrusted to them by Plaintiff and the Class for their care and treatment.

90. Defendants knowingly received, accepted, and appreciated the benefits conferred upon them by Plaintiff and the Class.

91. The fees for health care services that Plaintiff and the Class paid to Defendants were supposed to be used by Defendants, in part, to pay for the administrative costs of data management and security used to safeguard the Personal Information of Plaintiff and the Class.

92. Defendants failed to secure Plaintiff's and Class Members' Personal Information, and, therefore, did not provide full compensation for the benefit Plaintiff and the Class provided.

93. Under principals of equity and good conscience, it would be unjust and unfair for Defendants to retain money belonging to Plaintiff and the Class because Defendants failed to implement data management and security measures mandated by HIPAA and FTC guidelines, dispose of Personal Information that was no longer needed or required, and timely and accurately inform Plaintiff and the Class of the Data Breach.

94. As a result of Defendants conduct, Plaintiff and the Class suffered damages in the amount of the difference between the price they paid for Defendants' services as promised and the actually diminished value of its health care services and the costs of future monitoring of their credit history for identity theft and fraud.

95. Plaintiff, on behalf of herself and the other members of the Class, seeks disgorgement of the money that Defendants unjustly received plus prejudgment interest, and costs.

## COUNT IV

## BREACH OF FIDUCIARY DUTY

96. Plaintiff incorporates paragraphs 1 through 57 as if fully stated herein.

97. In light of their special and private relationship which requires Plaintiff and Class Members to share intimate medical information with Defendants, Defendants have become guardians of that information. As guardians, Defendants owed a fiduciary duty to Plaintiff and the Class to protect their Personal Information and keep them apprised of when that information becomes exposed or compromised in a timely manner.

98. Defendants breached their fiduciary duty by failing to comply with the guidelines outlined under HIPAA and by the FTC for safeguarding and storing Personal Information. This failure resulted in the Data Breach.

99. Defendants further breached their fiduciary duty by failing to dispose of Personal Information that was no longer needed or required, which unnecessarily exposed more patients to the Data Breach, and by failing to timely and accurately inform Plaintiff and the Class Members of the Data Breach, which recklessly delayed mitigation efforts.

100. As a direct and proximate cause of Defendants' breaches of their fiduciary duty, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (a)

the compromise, publication, theft, and /or unauthorized use of their Personal Information: (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 Personal Information, which remains in the possession of Defendants and is subject to further breaches so long as Defendants fail to undertake appropriate measures to protect Personal Information in their 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 remained of the lives of Plaintiff and the impacted patients.

101. Plaintiff, on behalf of herself and the other Members of the Class, seeks compensatory damages for breach of fiduciary duty, which entails the amount of the difference between the price they paid for Defendants' services as promised and the actually diminished value of its health care services and the costs of future monitoring of their credit history for identity theft and fraud, plus prejudgment interest, and costs.

## COUNT V

## INVASION OF PRIVACY

102. Plaintiff incorporates paragraphs 1 through 57 as if fully stated herein.

103. Plaintiff and the Class had a legitimate expectation of privacy regarding their medical and reproductive histories and were accordingly entitled to the protection of this information against disclosure to unauthorized third parties.

104. Defendants owed a duty to its patients, including Plaintiff and the Class, to keep this information confidential.

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

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

107. The Data Breach constitutes an intentional interference with Plaintiff's and Class Members' 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.

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

109. Defendants acted with a knowing state of mind when they retained patient medical records longer than required, thereby unnecessarily exposing those records to the Data Breach.

110. Defendants acted with a knowing state of mind when they failed to notify Plaintiff and the Class in a timely fashion about the Data Breach, thereby recklessly delaying mitigation efforts.

111. Acting with knowledge, Defendants had notice and knew that their inadequate cybersecurity practices would cause injury to Plaintiff and the Class.

112. As a proximate result of Defendants' acts and omissions, the private medical records of Plaintiff and Class Members were stolen by a third party and now available to disclosure to others without authorization, causing Plaintiff and the Class to suffer damages.

113. Unless and until enjoined and restrained by order of this Court, Defendants' wrongful conduct will continue to cause great and irreparable injury to Plaintiff and the Class since those medical records are still maintained by Defendants with their inadequate cybersecurity system and policies.

114. Plaintiff and the Class have no adequate remedy at law for the injuries relating to Defendants' continued possession of their medical records. A judgment for monetary damages will not end Defendants' inability to safeguard the medical records of Plaintiff and the Class.

115. In addition to injunctive relief, Plaintiff, on behalf of herself and the other members of the Class, also seeks compensatory damages for Defendants invasion of privacy, which entails the costs of future monitoring of their credit history for identity theft and fraud, plus prejudgment interest, and costs.

## COUNT VI

### VIOLATION OF ILLINOIS CONSUMER FRAUD ACT – 815 ILCS § 505/2 (Illinois Class only)

116. Plaintiff incorporates paragraphs 1 through 57 as if fully stated herein.

117. ICFA is a "regulatory and remedial statute intended to protect consumers, borrowers, and business persons against fraud, unfair methods of competition, and other unfair and deceptive business practices." *Robinson v. Toyota Motor Credit Corp.*, 201 Ill.2d 403, 416-17 (2002); *Hill v. PS Illinois Trust,* 368 Ill.App.3d 310, 319 (1st Dist. 2006). It is to be liberally construed to effectuate its purpose. *Robinson*, 201 Ill.2d at 417.

118. Recovery under ICFA may be had for unfair as well as deceptive conduct. *Robinson*, 201 Ill.2d at 417. In determining whether conduct is unfair under the Act, courts consider (1) whether the practice offends public policy; (2) whether it is oppressive, immoral, unethical, or unscrupulous; and (3) whether it causes consumers substantial injury. *Boyd v. U.S. Bank, N.A.*, 787 F. Supp. 2d 747, 751 (N.D. Ill. 2011); *Dubey v. Public Storage, Inc.*, 395 Ill.App.3d 342, 354 (1st Dist. 2009). A practice can be unfair without meeting all three criteria. *Id.*

119. A practice offends public policy "if it violates a standard of conduct contained in an existing statute or common law doctrine that typically applies to such a situation." *Boyd*, 787 F. Supp. 2d at 752; *Beatty v. Accident Fund General Insurance Co.*, 2018 WL 3219936, at *12 (S.D. Ill. 2018). In other words, a plaintiff may base an ICFA claim on violations of other statutes or regulations, which alone do not allow for private enforcement. *Boyd*, 787 F. Supp. 2d at 752. Accordingly, "[v]iolations of agency directives … can be a hallmark of unfairness under ICFA." *Id.* at 753.

120. Here, Defendants' conduct is unfair under ICFA. First, Defendants violated numerous DHS regulations regarding HIPAA guidelines for safeguarding Personal Information. In allowing the Data Breach to occur, Defendants failed to: (a) ensure the confidentiality, integrity, and availability of all electronic protected health information the entity creates, receives, maintains, or transmits (45 C.F.R. § 164.306(a)(1)); (b) protect against any reasonably anticipated threats or hazards to the security or integrity of such information (45 C.F.R. § 164.306(a)(2)); (c) protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required (45 C.F.R. § 164.306(a)(3)); (d) implement policies and procedures to prevent, detect, contain, and correct security violations (45 C.F.R. § 164.308(1)); (e) implement

technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights (45 C.F.R. § 164.312(a)(1)); (f) have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information (45 C.F.R. § 164.530(c)(1)); and (g) mitigate, to the extent practicable, any harmful effect that is known of a use or disclosure of protected health information (45 C.F.R. § 164.530(f)). Accordingly, Defendants' inability to safeguard Plaintiff's and Class Members' Personal Information offends public policy.

121. Second, Defendants' conduct against Plaintiff and the Class is oppressive in that Plaintiff and the Class had no choice but share their Personal Information with Defendants in order to proceed with their quest to have a child. On information and belief, all fertility clinics require this information. Moreover, Plaintiff and the Class were assured by Defendants that their Personal Information would be secured.

122. And third, Defendants' failure to safeguard Plaintiff's and Class Members' Personal Information and leaving it exposed to cybercriminals and other unauthorized actors constitutes a substantial injury in that Plaintiff and the Class will not only have to spend the remainder of their lives at greater risk for identity theft and fraud (having to constantly monitor for the same), but also live with the knowledge that their most intimate medical details are subject to public view.

123. Additionally, Defendants violated FTC guidelines by failing to: promptly dispose of Personal Information when no longer required to be stored; encrypt information stored on computer networks; understand vulnerabilities of its network; implement policies to correct security problems; use an intrusion detection system to expose a breach as soon as it occurs;

monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach. These failures constitute unfair acts or practices, subjecting them to an ICFA claim. 15 U.S.C. § 45.

124. Finally, Defendants violated PIPA by failing to immediately notify Plaintiff and the Class that their Personal Information was exposed during the Data Breach. 815 ILCS § 530/10 (a) and (b). This too constitutes an unlawful practice under ICFA. 815 ILCS 530/20.

125. In sum, Defendants' numerous failures in safeguarding Plaintiff's and Class Members' Personal Information violates ICFA.

126. As a result, 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 Personal Information: (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 the publication of their Personal Information, which remains in the possession of Defendants and is subject to further breaches so long as Defendants fail to undertake appropriate measures to protect Personal Information in their 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 Classes.

127. Defendants' failure to safeguard Plaintiff's and Class Members' Personal Information in violation of HIPAA and FTC guidelines and PIPA was the direct and proximate cause of damages incurred by Plaintiff and the Class.

128. Accordingly, Plaintiff, on behalf of herself and the other members of the Classes, seeks compensatory damages for the costs of future monitoring of their credit history for identity theft and fraud, plus prejudgment interest, and costs as provided by 818 ILCS § 505/10(a) and, in the event that Defendants violations are found to be willful, punitive damages. *Id.*

**WHEREFORE**, Plaintiff, individually and on behalf of the other members of the Classes, demands judgment in her favor and against Defendants, US FERTILITY, LLC and FERTILITY CENTERS OF ILLINOIS, S.C., jointly and severally, as follows:

A. That the Court adjudge and decree that the present case may be properly maintained as a class action, appoint Plaintiff as the representative of the Class, and appoint Plaintiff's counsel as counsel for the Class;

B. That the Court award the aggregate actual damages of Plaintiff and of the other members of the Class who had their Personal Information exposed during the Data Breach;

C. That the Court enjoin Defendants from exposing Plaintiff's and Class Members' Personal Information to future Data Breaches through their failure to properly safeguard that information;

D. That the Court award prejudgment interest and punitive damages;

E. That the Court award reasonable attorneys' fees and costs; and

F. That the Court grant such further relief as it deems just.

**JURY DEMAND**

Plaintiff demands a trial by jury of all claims in this Class Action Complaint so triable.

**NOTICE TO THE ILLINOIS ATTORNEY GENERAL**

A copy of this Complaint will be mailed to the Illinois Attorney General.

Respectfully Submitted,

JANE DOE, individually and as the representative of a class of similarly-situated persons

By: /s/ Ross M. Good
Ross M. Good
One of her attorneys

Ross M. Good
Patrick J. Solberg
ANDERSON + WANCA
3701 W. Algonquin Rd. Ste 500
Rolling Meadows, IL 60008
Telephone: (847) 368-1500
rgood@andersonwanca.com
psolberg@andersonwanca.com