UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND
SOUTHERN DIVISION

ALEC VINSANT[1]
c/o: Murphy Falcon Murphy
1 South Street, 30th Floor
Baltimore, MD 21202

and

MARLA VINSANT
c/o: Murphy Falcon Murphy
1 South Street, 30th Floor
Baltimore, MD 21202

Individually and on behalf of all others similarly situated,

Plaintiffs,

v.

US FERTILITY, LLC, (a Montgomery County, Maryland Resident)
9600 Blackwell Road, Suite 500
Rockville, MD 20850

s/o: The Corporation Trust Inc.
2405 York Road, Suite 201
Lutherville, MD 21093

Defendant.

Civil Action No.

CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

(1) Negligence
(2) Breach of Implied Contract
(3) Unjust Enrichment
(4) Nevada Deceptive Trade Practices Act

CLASS ACTION COMPLAINT

Plaintiffs Alec Vinsant and Marla Vinsant, individually, and on behalf of all others similarly situated, upon personal knowledge of the facts pertaining to them and based on

[1] Due to the nature of the claims regarding breach of personally identifying information Plaintiffs who are residents of the State of Texas will request that the Court grant them permission to shield their address in a subsequent pleading; but will provide this information to Defendants.

the investigation of their counsel, hereby bring this Class Action Complaint against Defendant US Fertility, LLC ("USF" or "Defendant"), and allege as follows:

INTRODUCTION AND NATURE OF THE CASE

1. Plaintiffs bring this class action against USF on behalf of themselves and all other persons harmed by the September 2020 ransomware attack and data breach that affected patients of fertility clinics (the "Data Breach").

2. USF is one of the largest support services networks for fertility clinics in the United States, providing administrative, clinical, and business information services.

3. Unfortunately, USF did not keep its patient data secure. From August 12, 2020 through September 14, 2020, hackers gained access to a vast trove of personal identifying information from the Data Breach, including names, dates of birth, addresses, Social Security numbers, driver's license and state ID numbers, passport numbers, medical treatment/diagnosis information, medical record information, health insurance and claims information, credit and debit card information, and financial account information (collectively, "PII").

4. Instead of immediately notifying patients that their PII had been exfiltrated, USF waited over two months. It was not until around November 2020 that USF began notifying patients of the fertility clinics using its services that its systems had been compromised by a ransomware attack. USF explained to patients that hackers exfiltrated their sensitive data before USF became aware of the attack.

5. Infertility is particularly sensitive and private and those going through treatments to have a baby have reasonable expectations that their PII will be protected and remain confidential. Accordingly, this data security breach is particularly egregious to the victims identified herein.

6. USF's carelessness and inadequate data security caused patients of fertility clinics utilizing its services to lose all sense of privacy. Consequently, Plaintiffs and Class

members have suffered irreparable harm and are subject to an increased risk of identity theft. Plaintiffs' and Class members' PII has been compromised and they must now undertake additional security measures and precautions to minimize their risk of identity theft and emotional devastation.

7. The Data Breach was the result of USF's inadequate and laxed approach to the data security and protection of its customers' PII that it collected during business.

8. Plaintiffs' and the Class members' rights were disregarded by USF's reckless and/or negligent failure to take adequate and reasonable measures to ensure its data systems were protected, failure to disclose the material fact that it did not have adequate computer systems and security practices to safeguard PII, failure to take available steps to prevent the Data Breach, and failure to monitor and timely detect the Data Breach.

9. As a result of the Data Breach, Plaintiffs', and Class members' PII has been exposed to criminals for misuse. The injuries Plaintiffs and the Class suffered or may suffer as a direct result of the Data Breach include:

a. Theft of medical, personal and financial information;
b. Unauthorized charges on debit and credit card accounts;
c. Costs associated with the detection and prevention of identity theft and unauthorized use of financial accounts;
d. Damages arising from the inability to use debit or credit card accounts because accounts were suspended or otherwise rendered unusable because of fraudulent charges stemming from the Data Breach;
e. Damages arising from the inability to withdraw or otherwise access funds because accounts were suspended, restricted, or otherwise rendered unusable as a result of the Data Breach, including, but not limited to, missed bill and loan payments, late-payment charges, and lowered credit scores and other adverse impacts on credit;
f. Costs associated with spending time to address and mitigate the actual and future consequences of the Data Breach such as finding fraudulent charges, cancelling and

reissuing payment cards, purchasing credit monitoring and identity theft protection services, imposition of withdrawal and purchase limits on compromised accounts, including, but not limited to, lost productivity and opportunities, time taken from the enjoyment of one's life, and the inconvenience, nuisance and annoyance of dealing with all issues resulting from the Data Breach;

g. The imminent and impending injury resulting from the potential fraud and identity theft posed by PII being exposed for theft and sale on the dark web; and

h. The loss of Plaintiffs' and Class members' privacy.

10. The injuries Plaintiffs and the Class suffered were directly and proximately caused by USF's failure to implement or maintain adequate data security measures for PII.

11. Plaintiffs and the Class members retain a significant interest in ensuring that their PII, which remains in USF's possession, is protected from further breaches, and seek to remedy the harms suffered as a result of the Data Breach for themselves and on behalf of similarly situated consumers whose PII was stolen.

JURISDICTION AND VENUE

12. This Court has jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million, exclusive of interest and costs. At least one member of the Class, defined below, is a citizen of a different state than Defendant, and there are more than 100 putative Class members.

13. This Court has personal jurisdiction over Defendant because it maintains its principal place of business in this District, is registered to conduct business in Maryland, and has sufficient minimum contacts with Maryland.

14. Venue is proper in this District under 28 U.S.C. § 1391(b)(2) because a substantial part of the events or omissions giving rise to the claim occurred in this District.

PARTIES

15. Plaintiff Alec Vinsant is a citizen of the State of Texas and resides in Sulphur Springs, Texas.

16. Plaintiff Marla Vinsant is a citizen of the State of Texas and resides in Sulphur Springs, Texas.

17. Plaintiffs Alec and Marla Vinsant, who previously resided in Nevada, formerly sought treatment at the Nevada Center for Reproductive Medicine, which contracts with USF for IT platforms and services. Plaintiffs Alec and Marla Vinsant received a notice from USF dated January 8, 2021 ("Notice Letter"). The Notice Letter informed them of the Data Breach and that their PII had been exposed to unauthorized third parties.

18. In October 2020, Plaintiff Alec Vinsant discovered that someone had used his Social Security number to fraudulently apply for unemployment benefits in Nevada.

19. Upon discovering the fraudulent application for unemployment benefits, Alec filed a complaint with the Federal Trade Commission, filed an Internet crime complaint with the FBI and filed a claim with the Social Security Administration. He also filed a fraud report with the Nevada Department of Employment, Training and Rehabilitation and requested they stop and flag the fraudulent claim. Alec also checked and continues to monitor his credit report.

20. In December 2020, Plaintiff Marla Vinsant, who ordinarily has a credit score over 800, noticed that her credit score dropped 50 points.

21. Defendant US Fertility, LLC is incorporated in the State of Delaware and maintains its principal place of business in Rockville, Maryland. USF provides administrative, clinical, and business information solutions to fertility clinics across the United States.

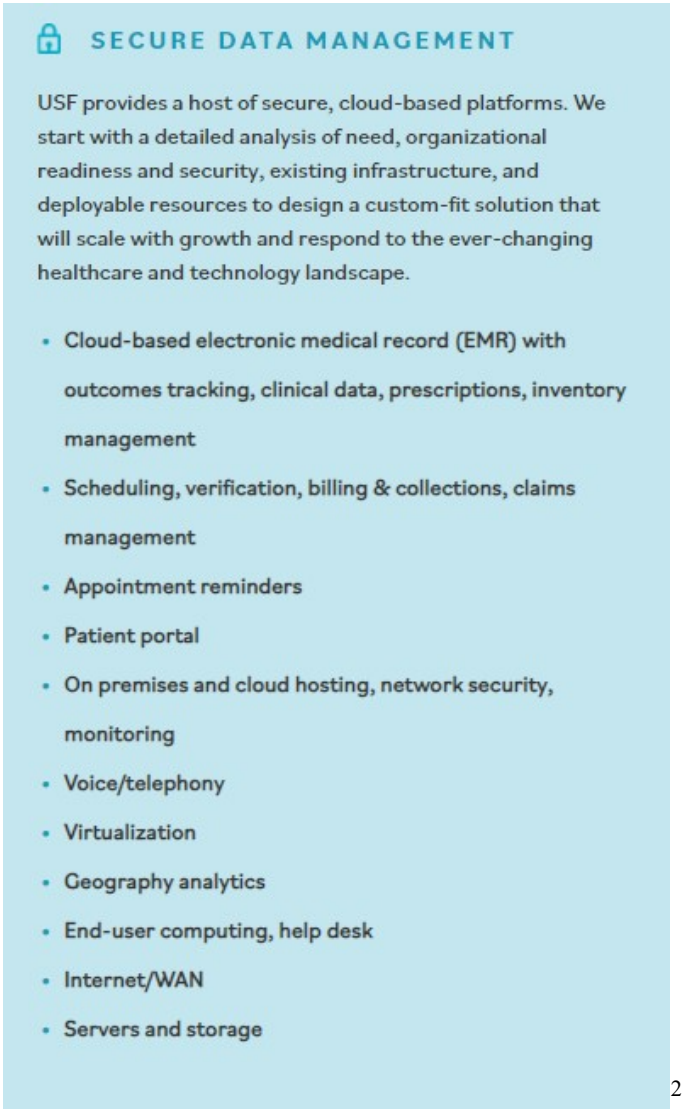
22. US Fertility, LLC is a joint venture that was formed in May 2020 between Shady Grove Fertility, a fertility clinic with a number of locations on the East Coast, and

Amulet Capital Partners, a private equity firm that invests primarily in the healthcare industry. U.S. Fertility has over 50 locations in the United States.

FACTUAL BACKGROUND

A. The Ransomware Attack and Data Breach

23. USF markets itself on its website as providing "Secure Data Management" with a "secure suite" of professional management services for fertility clinics.



[2]

[2] https://www.usfertility.com/physicians/practice-success/ (last visited January 21, 2021).

24. Despite its claims of data security, including "secure, cloud-based platforms," in August 2020 Defendant allowed hackers to access its systems and exfiltrate sensitive patient data.

25. In mid-November 2020, USF began notifying patients of its network of fertility clinics that it had succumbed to a ransomware attack. According to USF, unauthorized individuals gained access to its systems on August 12, 2020, with access continuing until September 14, 2020, when it discovered the ransomware attack. Prior to deployment of the ransomware, hackers were able to acquire files including patients' PII from USF's servers.

26. The data exfiltrated included sensitive patient data, including names, dates of birth, addresses, Social Security numbers, driver's license and state ID numbers, passport numbers, medical treatment and diagnosis information, medical record information, health insurance and claims information, credit and debit card information, and financial account information.

27. USF maintained Plaintiffs' and Class Members' PII on cloud-based platforms, which were not secure enough to ward off ransomware attacks. Despite widely-reported cyberattacks on businesses in the healthcare industry over the course of recent years, USF failed to maintain adequate security of Plaintiffs' and Class Members' data to protect against cyberattacks and the ransomware that infiltrated their system(s).

B. The Data Breach Was Entirely Avoidable and Foreseeable

28. USF could have prevented the Data Breach from occurring. USF failed to take adequate and reasonable measures to ensure its computer/server systems were protected against unauthorized access and failed to take actions that could have stopped the Data Breach before it occurred.

29. USF failed to disclose to Plaintiffs and Class members that its computer/server systems and security practices were inadequate to reasonably safeguard their PII and failed to immediately notify them of the data theft.

30. As a direct result of USF's conduct, Plaintiffs and Class members were injured.

31. USF was at all times fully aware of its obligations under federal and state laws and various standards and regulations to protect data entrusted to it.

32. Despite its awareness of its data protection obligations, USF's treatment of the PII entrusted to it by Plaintiffs and Class members fell short of satisfying its legal duties and obligations. USF failed to ensure that access to its computer/server systems were reasonably safeguarded, particularly against ransomware attacks.

C. Data Breaches Lead to Identity Theft and Cognizable Injuries

33. The information exposed by USF is a virtual goldmine for phishers, hackers, identity thieves and cyber criminals.

34. Stolen PII is often trafficked on the "dark web," a heavily encrypted part of the Internet that is not accessible via traditional search engines. Law enforcement has difficulty policing the "dark web" due to this encryption, which allows users and criminals to conceal identities and online activity.

35. The PII of consumers remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from $40 to $200.[3]

36. Social Security numbers are among the worst kind of personal information to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change. The Social Security Administration stresses that the loss of an individual's Social Security number, as is the case here, can lead to identity theft and extensive financial fraud:

[3] *Your personal data is for sale on the dark web. Here's how much it costs*, Digital Trends, Oct. 16, 2019, available at: https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last accessed Jan. 21, 2021).

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.[4]

37. What's more, it is no easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

38. Even then, a new Social Security number may not be effective. According to Julie Ferguson of the Identity Theft Resource Center, "The credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[5]

39. Medical data is also especially valuable to identity thieves. According to a 2012 Nationwide Insurance report, "[a] stolen medical identity has a $50 street value..."[6] In fact, the medical industry has experienced disproportionally higher instances of data theft than any other industry.

40. Medical identity theft is one of the forms of identity theft that is most common, most expensive, and most difficult to prevent. According to Kaiser Health News, "medical-related identity theft accounted for 43 percent of all identity thefts reported in the

---

[4] Social Security Administration, *Identity Theft and Your Social Security Number*, available at: https://www.ssa.gov/pubs/EN-05-10064.pdf (last visited Jan. 21, 2021).
[5] Bryan Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), available at: http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millionsworrying-about-identity-theft (last visited Jan. 21, 2021).
[6] Study: Few Aware of Medical Identity Theft Risk, Claims Journal, https://www.claimsjournal.com/news/national/2012/06/14/208510.htm (last visited Jan. 21, 2021).

United States in 2013," which is more "than identity thefts involving banking and finance, the government and the military, or education."[7]

41. As indicated by Jim Trainor, second in command at the FBI's cyber security division: "Medical records are a gold mine for criminals – they can access a patient's name, DOB, Social Security and insurance numbers, and even financial information all in one place."[8]

42. Because of this, the information compromised in the Data Breach here is more valuable than the loss of, for example, credit card information in a retailer data breach. There, victims can cancel or close credit and debit card accounts. Here, the information compromised in this Data Breach—Social Security number, prescription information, name, date of birth, and addresses—is impossible to "close" and difficult, if not impossible, to change.

43. The data stolen in this case commands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information, personally identifiable information and Social Security numbers are worth more than 10 times on the black market."[9]

44. Once PII is sold, it is often used to gain access to various areas of the victim's digital life, including bank accounts, social media, credit card, and tax details. This can

---

[7] Michael Ollove, "The Rise of Medical Identity Theft in Healthcare," Kaiser Health News, Feb. 7, 2014, https://khn.org/news/rise-of-indentity-theft/ (last visited Jan. 21, 2021).

[8] IDExperts, *You Got It, They Want It: Criminals Targeting Your Private Healthcare Data, New Ponemon Study Shows*, https://www.idexpertscorp.com/knowledge-center/single/you-got-it-they-want-it-criminals-are-targeting-your-private-healthcare-dat (last visited Jan. 21, 2021).

[9] Time Greene, Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers, IT World, (Feb. 6, 2015), available at: https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last visited Jan. 21, 2021).

lead to additional PII being harvested from the victim, as well as PII from family, friends, and colleagues of the original victim.

45. 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 in 2019, resulting in more than $3.5 billion in losses to individuals and business victims.

D. USF was on Notice of Data Breach Threats and the Inadequacy of its Security

46. USF was on notice that companies in the healthcare industry are targets for cyberattacks.

47. In August 2014, after a cyberattack on Community Health Systems, Inc., the FBI warned companies within the healthcare industry that hackers were targeting them. The warning stated that "[t]he FBI has observed malicious actors targeting healthcare related systems, perhaps for the purpose of obtaining the Protected Healthcare Information (PHI) and/or Personally Identifiable Information (PII)."[10]

48. The American Medical Association ("AMA") has also warned healthcare companies about the importance of protecting their patients' confidential information:

> Cybersecurity is not just a technical issue; it's a patient safety issue. AMA research has revealed that 83% of physicians work in a practice that has experienced some kind of cyberattack. Unfortunately, practices are learning that cyberattacks not only threaten the privacy and security of patients' health and financial information, but also patient access to care.[11]

[10] Jim Finkle, *FBI Warns Healthcare Firms that they are Targeted by Hackers*, Reuters (Aug. 2014), https://www.reuters.com/article/us-cybersecurity-healthcare-fbi/fbi-warns-healthcare-firms-they-are-targeted-by-hackers-idUSKBN0GK24U20140820 (last visited Jan. 21, 2021).

[11] Andis Robeznieks, Cybersecurity: Ransomware attacks shut down clinics, hospitals, Am. Med. Ass'n (Oct. 4, 2019), https://www.ama-assn.org/practice-management/sustainability/cybersecurity-ransomware-attacks-shut-down-clinics-hospitals (last visited Jan. 21, 2021).

49. USF was on notice that the federal government has been concerned about healthcare company data encryption. USF knew it kept protected health and personal information in its computer systems and yet did not encrypt its computer systems.

50. The United States Department of Health and Human Services' Office for Civil Rights urges the use of encryption of data containing sensitive personal information. As long ago as 2014, the Department fined two healthcare companies approximately two million dollars for failing to encrypt laptops containing sensitive personal information. In announcing the fines, Susan McAndrew, the DHHS's Office of Human Rights' deputy director of health information privacy, stated "[o]ur message to these organizations is simple: encryption is your best defense against these incidents."[12]

E. USF Failed to Comply with Federal Trade Commission Requirements

51. Federal and State governments have established security standards and issued recommendations to minimize data breaches and the resulting harm to individuals and financial institutions. The Federal Trade Commission ("FTC") has issued numerous guides for businesses that highlight the importance of reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[13]

52. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established guidelines for fundamental data security principles and practices for business.[14] Among other things, the guidelines note businesses

[12] *Stolen Laptops Lead to Important HIPAA Settlements*, U.S. Dep't of Health and Human Services (Apr. 22, 2014), available at https://wayback.archive-it.org/3926/20150618190135/http://www.hhs.gov/news/press/2014pres/04/20140422b.html (last visited Oct. 30, 2020).

[13] See Federal Trade Commission, *Start With Security* (June 2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last visited Jan. 21, 2021).

[14] See Federal Trade Commission, Protecting Personal Information: A Guide for Business (Oct. 2016), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited Jan. 21, 2021).

should properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct security problems. The guidelines also recommend 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.[15]

53. Additionally, the FTC recommends that companies limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.[16]

54. Highlighting the importance of protecting against data breaches, the FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect PII, treating 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 of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.[17]

55. By allowing an unknown third party to access a USF server, USF failed to employ reasonable and appropriate measures to protect against unauthorized access to confidential employee data. USF's data security policies and practices constitute unfair acts or practices prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

---

[15] *Id.*
[16] Federal Trade Commission, *Start With Security*, *supra* note 12.
[17] Federal Trade Commission, Privacy and Security Enforcement Press Releases, https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/privacy-security-enforcement (last visited Jan. 21, 2021).

F. Plaintiffs and Class Members Have Suffered Ascertainable Losses, Economic Damages, and Other Actual Injury and Harm

56. As a direct and proximate result of USF's wrongful actions, inaction and/or omissions, the resulting Data Breach, and the unauthorized release and disclosure of Plaintiffs' and other Class members' PII, Plaintiffs and the other Class members have suffered, and will continue to suffer, ascertainable losses, economic damages, and other actual injury and harm, including, *inter alia*:

a. The compromise, publication, theft, and/or unauthorized use of their PII;

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

d. 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 Plaintiffs and Class members.

57. In addition to a remedy for the economic harm, Plaintiffs and Class members maintain an undeniable interest in ensuring that their PII is secure, remains secure, and is not subject to further misappropriation and theft.

58. To date, other than providing 12 months of credit monitoring and identity protection services, USF does not appear to be taking any measures to assist Plaintiffs and the Class members.

CLASS DEFINITIONS AND ALLEGATIONS

59. Pursuant to Federal Rules of Civil Procedure 23(b)(2), (b)(3) and (c)(4), Plaintiffs seek certification of the following national class ("Nationwide Class"):

> All persons residing in the United States whose PII was accessed during the Data Breach that affected USF's network that took place between August 2020 and September 2020.

60. Pursuant to Federal Rules of Civil Procedure 23(b)(2), (b)(3) and (c)(4), Plaintiffs seek certification of the following Nevada state class ("Nevada Class"):

> All persons residing in Nevada whose PII was accessed during the Data Breach that affected USF's network that took place between August 2020 and September 2020.

61. The Nationwide Class and Nevada Class are collectively referred to herein as "Class" unless otherwise stated.

62. Excluded from the proposed Class is Defendant, including any entity in which Defendant has a controlling interest, is a subsidiary, or which is controlled by Defendant, as well as the officers, directors, affiliates, legal representatives, heirs, predecessors, successors, and assigns of Defendant.

63. Plaintiffs reserve the right to amend or modify the class definitions with greater specificity or division, or create and seek certification of additional classes, after having had an opportunity to conduct discovery.

64. **Numerosity**: Although the exact number of Class members is uncertain and can only be ascertained through appropriate discovery, the number is great enough – with the Data Breach impacting, on information and belief, tens of thousands of individuals - such that joinder is impracticable. The disposition of the claims of these Class members in a single action will provide substantial benefits to all parties and to the Court. The Class members may be identifiable from objective means, such as information and records in Defendant's possession, custody, or control.

65. **Commonality and Predominance:** Common questions of law and fact exist as to the proposed Class members and predominate over questions affecting only individual Class members. These common questions include:

a. Whether Defendant engaged in the wrongful conduct alleged herein;

b. Whether Defendant's data security measures to protect Plaintiffs' and Class member's PII were reasonable in light of FTC data security recommendations, and best practices recommended by data security experts;

c. Whether Defendant's failure to implement adequate data security measures resulted in or was the proximate cause of the Data Breach;

d. Whether Defendant's conduct, including its failure to act, resulted in or was the proximate cause of the Data Breach, resulting in the loss of PII of Plaintiffs and Class members;

e. Whether Defendant owed a legal duty to Plaintiffs and Class members to exercise due care in collecting, storing, and safeguarding their PII;

f. Whether Defendant negligently or recklessly breached legal duties owed to Plaintiffs and the other Class members to exercise due care in collecting, storing, and safeguarding their PII;

g. Whether Plaintiffs and the other Class members are entitled to actual, statutory, or other forms of damages, and other monetary relief; and

h. Whether Plaintiffs and the other Class members are entitled to equitable relief, including, but not limited to, injunctive relief and restitution.

66. **Typicality:** Plaintiffs' claims are typical of the claims of the Class members. All Class members were subject to the Data Breach and had their PII accessed by and/or disclosed to unauthorized third parties.

67. **Adequacy of Representation:** Plaintiffs are adequate representatives of the Class because their interests do not conflict with the interests of the other Class members they seek to represent; they have retained counsel competent and experienced in complex

class action litigation, and Plaintiffs will prosecute this action vigorously. The interests of the Class will be fairly and adequately protected by Plaintiffs and their counsel.

68. **Superiority:** A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this matter as a class action. The damages, harm, or other financial detriment suffered individually by Plaintiffs and the other Class members are relatively small compared to the burden and expense that would be required to litigate their claims on an individual basis against Defendant, making it impracticable for Class members to individually seek redress for Defendant's wrongful conduct. Even if Class members could afford individual litigation, the court system could not. Individualized litigation would create a potential for inconsistent or contradictory judgments and increase the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single court.

COUNT 1
Negligence

69. Plaintiffs incorporate by reference all allegations in this Complaint as though fully set forth herein.

70. Defendant owed a duty to Plaintiffs and the Class to exercise reasonable care in obtaining, securing, safeguarding, storing, and protecting Plaintiffs' and Class members' PII from being compromised, lost, stolen, and accessed by unauthorized persons. This duty includes, among other things, designing, maintaining, and testing its data security systems to ensure that Plaintiffs' and Class members' PII in Defendant's possession was adequately secured and protected.

71. Defendant owed a duty of care to Plaintiffs and members of the Class to provide security, consistent with industry standards, to ensure that its systems and networks adequately protected the PII of Plaintiffs and Class members.

72. Defendant owed a duty of care to Plaintiffs and members of the Class because they were foreseeable and probable victims of any inadequate data security practices. Defendant knew or should have known of the inherent risks in collecting and storing the PII of Plaintiffs and Class members and the critical importance of adequately securing such information.

73. Plaintiffs and members of the Class entrusted Defendant with their PII with the understanding that Defendant would safeguard their information, and Defendant was in a position to protect against the harm suffered by Plaintiffs and members of the Class as a result of the Data Breach.

74. Defendant's own conduct also created a foreseeable risk of harm to Plaintiffs and Class members. Defendant's misconduct included failing to implement the systems, policies, and procedures necessary to prevent the Data Breach.

75. Defendant knew, or should have known, of the risks inherent in collecting and storing PII and the importance of adequate security. Defendant knew about – or should have been aware of - numerous, well-publicized data breaches, including ransomware attacks, affecting businesses in the United States.

76. Defendant breached its duties to Plaintiffs and Class members by failing to provide reasonable or adequate computer systems and data security to safeguard the PII of Plaintiffs and Class members.

77. Because Defendant knew that a breach of its systems would potentially damage hundreds of thousands of patients, including Plaintiffs and Class members, Defendant had a duty to adequately protect its data systems and the PII contained therein.

78. Plaintiffs and Class members reasonably believed that Defendant would take adequate security precautions to protect their PII.

79. Defendant also had independent duties under state and federal laws that required Defendant to reasonably safeguard Plaintiffs' and Class members' PII.

80. Through Defendant's acts and omissions, including Defendant's failure to provide adequate security and its failure to protect Plaintiffs' and Class members' PII from being foreseeably accessed, Defendant unlawfully breached its duty to use reasonable care to adequately protect and secure the PII of Plaintiffs and Class members during the time it was within Defendant's possession or control.

81. In engaging in the negligent acts and omissions as alleged herein, which permitted an unknown third party to exfiltrate Plaintiffs' and Class members' PII from Defendant's data systems, Defendant violated Section 5 of the FTC Act, which prohibits "unfair…practices in or affecting commerce." This prohibition includes failing to have adequate data security measures and failing to protect Plaintiffs' and Class members' PII.

82. Plaintiffs and the Class members are among the class of persons Section 5 of the FTC Act was designed to protect, and the injuries suffered by Plaintiffs and the Class members is the type of injury Section 5 of the FTC Act was intended to prevent. As a result, Defendant is negligent per se.

83. Neither Plaintiffs nor any of the Class members contributed to the Data Breach as described in this Complaint.

84. As a direct and proximate cause of Defendant's conduct, Plaintiffs and Class members have suffered and/or will suffer injury and damages, including: (i) the loss of the opportunity to determine for themselves how their PII is used; (ii) loss of their benefit of the bargain with Defendant; (iii) the publication and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (v) lost opportunity costs associated with effort expended and the loss of productivity 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 tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) anxiety, emotional distress, loss of privacy, and other economic and non-economic losses; (viii) the continued risk to

their PII, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect that PII in its continued possession; and, (ix) future costs in terms of time, effort and money that will be expended to prevent, detect, contest, and repair the inevitable and continuing consequences of compromised PII for the rest of their lives.

COUNT 2
Breach of Implied Contract

85. Plaintiffs incorporate by reference all allegations in this Complaint as though fully set forth herein.

86. Plaintiffs and Class members entered into an implied contract with Defendant by providing their PII to Defendant and/or Defendant's network of fertility clinics in exchange for healthcare services. Implied in these exchanges was a promise by Defendant to implement reasonable procedures and practices to protect the PII of Plaintiffs and Class members and to timely notify them in the event their PII was compromised.

87. Plaintiffs and Class members reasonably expected that Defendant had implemented adequate security measures to protect their PII and would allocate a portion of the money paid by Plaintiffs and Class members under the implied contracts to fund those security measures.

88. Neither Plaintiffs nor Class members would have provided their PII to Defendant or its network of fertility clinics for services without the implied contract between them and Defendant. Defendant needed to adequately safeguard Plaintiffs' and Class members' PII and provide timely notice of a data breach to realize the intent of the parties. Fertility information is sensitive and often emotionally charged.

89. Plaintiffs and Class members performed their obligations under the implied agreements with Defendant. Conversely, Defendant breached its obligations under the implied contracts by (i) failing to implement reasonable security procedures and practices to protect Plaintiffs' and Class members' PII; (ii) enabling unauthorized access of PII by

third parties due to the inadequate security measures; and (iii) failing to provide timely notice of the Data Breach.

90. As a direct and proximate result of Defendant's breaches of implied contract, Plaintiffs and Class members did not get the benefit of their implied contract with Defendant and were injured as described in detail above.

COUNT 3
Unjust Enrichment

91. Plaintiffs incorporate by reference all allegations in this Complaint as though fully set forth herein.

92. Plaintiffs and members of the Class conferred a monetary benefit on Defendant. Specifically, Plaintiffs and Class members paid for services at fertility clinics which, in turn, pay Defendant for administrative, clinical, and business services, and provided and entrusted their PII to those fertility clinics and to Defendant.

93. In exchange, Plaintiffs and Class members should have received from Defendant their expected goods and services, such as the security of their PII, and should have been entitled to have Defendant protect their PII with adequate data security, and timely notice of the Data Breach.

94. Defendant appreciated, accepted and retained the benefit bestowed upon it under inequitable and unjust circumstances arising from Defendant's conduct toward Plaintiffs and Class members as described herein; Plaintiffs and Class members conferred a benefit on Defendant, and Defendant accepted or retained that benefit. Defendant profited from the services Plaintiffs and Class members paid for and used Plaintiffs' and Class members' PII for business purposes.

95. Defendant failed to secure Plaintiffs' and Class members' PII and therefore, did not provide full compensation for the monetary benefit Plaintiffs and Class members conferred on Defendant.

96. Defendant acquired the PII through inequitable means in that they failed to disclose the inadequate security practices previously alleged.

97. Had Plaintiffs and Class members known that Defendant would not secure their PII using adequate security, they would not have chosen to receive care from the fertility clinics that Defendant provides services.

98. Plaintiffs and Class members have no adequate remedy at law.

99. Under these circumstances, it would be unjust for Defendant to be permitted to retain any of the benefits that Plaintiffs and Class members conferred on it.

100. Under the principles of equity and good conscience, Defendant should not be permitted to retain the money belonging to Plaintiffs and Class.

COUNT 4
NEVADA DECEPTIVE TRADE PRACTICES ACT, Nev. Rev. Stat. Ann. §§ 598.0903 et seq.

101. Plaintiffs, individually and on behalf of the Nevada state class, repeat and allege Paragraphs 1-100, as if fully alleged herein.

102. Defendant advertised, offered, or sold goods or services in Nevada and engaged in trade or commerce directly or indirectly affecting the people of Nevada.

103. Defendant engaged in deceptive trade practices in the course of its business or occupation, in violation of Nev. Rev. Stat. §§ 598.0915 and 598.0923, including:

a. Knowingly making a false representation as to the characteristics, uses, and benefits of goods or services for sale in violation of Nev. Rev. Stat. § 598.0915(5);

b. Representing that goods or services for sale are of a particular standard, quality, or grade when Defendant knew or should have known that they are of another standard, quality, or grade in violation of Nev. Rev. Stat. § 598.0915(7);

c. Advertising goods or services with intent not to sell them as advertised in violation of Nev. Rev. Stat § 598.0915(9);

d. Failing to disclose a material fact in connection with the sale of goods or services in violation of Nev. Rev. Stat. § 598.0923(A)(2); and

e. Violating state and federal statutes or regulations relating to the sale of goods or services in violation of Nev. Rev. Stat. § 598.0923(A)(3).

104. Defendant's deceptive trade practices in the course of its business or occupation include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs and Nevada class members' PII, which was a direct and proximate cause of the Data Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs and Nevada class members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, and Nevada's data security statute, Nev. Rev. Stat. § 603A.210, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiffs and Nevada class members' PII, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Nevada class members' Personal Information, including duties imposed by the FTC Act,

15 U.S.C. § 45, and Nevada's data security statute, Nev. Rev. Stat. § 603A.210;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiffs' and Nevada class members' PII; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and class members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, and Nevada's data security statute, Nev. Rev. Stat. § 603A.210.

105. Defendant's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendant's data security and ability to protect the confidentiality of consumers' PII.

106. Had Defendant disclosed to Plaintiffs and class members or fertility clinics that its data systems were not secure and, thus, vulnerable to attack, Defendant would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Instead, Defendant received, maintained, and compiled Plaintiffs' and class members' PII as part of the services Defendant provided and for which Plaintiffs and class members paid without advising Plaintiffs and class members that Defendant's data security practices were insufficient to maintain the safety and confidentiality of Plaintiffs' and class members' PII. Accordingly, Plaintiff and the Nevada class members acted reasonably in relying on Defendant's misrepresentations and omissions, the truth of which they could not have discovered.

107. Defendant acted intentionally, knowingly, and maliciously to violate Nevada's Deceptive Trade Practices Act, and recklessly disregarded Plaintiff and Nevada class members' rights. Defendant's past data breaches and breaches within the hospitality industry put it on notice that its security and privacy protections were inadequate.

108. As a direct and proximate result of Defendant's deceptive trade practices, Plaintiff and Nevada class members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including loss of the benefit of their bargain with Defendant as they would not have paid Defendant for goods and services or would have paid less for such goods and services but for Defendant's violations alleged herein; losses from fraud and identity theft; costs for credit monitoring and identity protection services; time and expenses related to monitoring their financial accounts for fraudulent activity; time and money spent cancelling and replacing passports; loss of value of their PII; and an increased, imminent risk of fraud and identity theft.

109. Plaintiff and Nevada class members seek all monetary and non-monetary relief allowed by law, including damages, restitution, punitive damages, and attorneys' fees and costs.

REQUEST FOR RELIEF

WHEREFORE, Plaintiffs, individually, and on behalf of all others similarly situated, respectfully requests that the Court enter an order:

a. Certifying the proposed Class as requested herein;
b. Appointing Plaintiffs as Class Representatives and undersigned counsel as Class Counsel;
c. Finding that Defendant engaged in the unlawful conduct as alleged herein;
d. Enjoining Defendant's conduct and requiring Defendant to implement proper data security policies and practices, including:
    i. Prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;

ii. Requiring Defendant to protect, including through encryption, all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state, or local laws;

iii. Requiring Defendant to delete, destroy, and purge the PII of Plaintiffs and the Class members unless Defendant can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiffs and the Class members;

iv. Requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the personal identifying information of Plaintiffs' and the Class members' PII:

v. Requiring Defendant to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

vi. Requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring;

vii. Requiring Defendant to audit, test, and train its security personnel regarding any new or modified procedures;

viii. Requiring Defendant to segment data by, among other things, creating firewalls and access controls so that if one area of Defendant's network is compromised, hackers cannot gain access to other portions of Defendant's systems;

ix. Requiring Defendant to conduct regular database scanning and securing checks;

x. Requiring Defendant to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling PII, as well as protecting the PII of Plaintiffs and the Class members;

xi. Requiring Defendant to conduct internal training and education routinely and continually, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

xii. Requiring Defendant to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Defendant's policies, programs, and systems for protecting PII;

xiii. Requiring Defendant to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendant's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

xiv. Requiring Defendant to meaningfully educate all Class members about the threats that they face because of the loss of their confidential PII to third parties, as well as the steps affected individuals must take to protect themselves;

xv. Requiring Defendant to implement logging and monitoring programs sufficient to track traffic to and from Defendant's servers;

xvi. Requiring Defendant to design, maintain, and test its computer systems to ensure that PII in its possession is adequately secured and protected;

xvii. Requiring Defendant to disclose any future data breaches in a timely and accurate manner;

xviii. Requiring Defendant to implement multi-factor authentication requirements; and

xix. Requiring Defendant's employees to change their passwords on a timely and regular basis, consistent with best practices.

e. Awarding Plaintiffs and Class members damages;

f. Awarding Plaintiffs and Class members pre-judgment and post-judgment interest on all amounts awarded;

g. Awarding Plaintiffs and the Class members reasonable attorneys' fees, costs, and expenses; and

h. Granting such other relief as the Court deems just and proper.

JURY DEMAND

Plaintiffs, individually, and on behalf of all others similarly situated, hereby demand a trial by jury as to all matters so triable.

Respectfully submitted,

Dated: January 26, 2021

/s/ Nicholas A. Szokoly

Nicholas A. Szokoly, Esq. (Bar No. 28157)
MURPHY, FALCON & MURPHY, P.A.
One South Street, 30th Floor
Baltimore, MD 21202
Telephone: (410) 951-8744
Facsimile: (410) 539-6599
nick.szokoly@murphyfalcon.com

Gayle M. Blatt, *Pro Hac Vice forthcoming*
P. Camille Guerra, *Pro Hac Vice forthcoming*
Catherine M. McBain, *Pro Hac Vice forthcoming*
CASEY GERRY SCHENK FRANCAVILLA BLATT & PENFIELD, LLP
110 Laurel Street
San Diego, CA 92101
Telephone: (619) 238-1811
Facsimile: (619) 544-9232
gmb@cglaw.com
camille@cglaw.com
kmcbain@cglaw.com

Rosemary M. Rivas, *Pro Hac Vice forthcoming*
David M. Berger, *Pro Hac Vice forthcoming*
GIBBS LAW GROUP LLP
505 14th Street, Suite 1110
Oakland, California 94612
Telephone: (510) 350-9700
Facsimile: (510) 350-9701
rmr@classlawgroup.com
dmb@classlawgroup.com

Attorneys for Plaintiffs and the Class