UNITED STATES DISTRICT COURT
DISTRICT OF MARYLAND
SOUTHERN DIVISION

NIKITIA FOREST
14413 Livingston Road
Accokeek, MD. 20607
Prince George's County

and

DORIS MATTHEW,
3482 Aviary Way
Woodbridge VA 22192

on behalf of themselves and all others similarly situated,

Plaintiffs,

v.

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

Serve: The Corporation Trust Incorporated
2405 York Road, Suite 201
Lutherville-Timonium, MD 21093

Defendant.

Case No.:

CLASS ACTION COMPLAINT FOR:

1. Negligence;
2. Breach of implied contract;
3. Violations of the Maryland Personal Information Protection Act, Md. Comm. Code §§ 14-3501, *et seq.*;
4. Violations of the Maryland Consumer Protection Act, Md. Code. Ann., Cm. Law §§ 13-101, *et seq.*;
5. Violations of the Virginia Consumer Protection Act, Code of Virginia §§ 59.1-196, *et seq.*; and
6. Unjust enrichment

DEMAND FOR JURY TRIAL

Plaintiffs Nikitia Forest and Doris Matthew ("Plaintiffs"), by their undersigned counsel, bring this action on behalf of themselves and all others similarly situated against US Fertility, LLC ("Defendant" or "US Fertility"). Plaintiffs make the following allegations based on the investigation of their counsel, personal knowledge, and upon information and belief:

NATURE OF THE ACTION

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

2. As part of its business, US Fertility collects substantial amounts of personal and medical information 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 (collectively, "PII").

3. Plaintiffs and Class members were required to provide US Fertility and/or US Fertility's network of fertility clinics with their PII in exchange for receiving healthcare services, with the assurance that such information would be kept confidential and safe from unauthorized access.

4. 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.

5. This expectation was reinforced by promises made to Plaintiffs and Class members at clinics in Defendant's networks that their PII would be kept confidential and used only in accordance with publicly available privacy policies.

6. However, from August 12, 2020 through September 14, 2020, hackers gained access to Plaintiff and Class members' PII through a ransomware attack on US Fertility's systems (the "Data Breach").

7. Instead of immediately notifying patients that their PII had been exfiltrated, US

Fertility waited over two months until November 2020 to begin notifying affected patients of the Data Breach.

8. US Fertility explained to patients that hackers exfiltrated their sensitive data before US Fertility became aware of the attack.

9. US Fertility maintained patient PII in a negligent or reckless manner by storing it on its computer network in a condition it knew or should have known was vulnerable to cyberattacks and US Fertility failed to disclose that it did not have adequately robust computer systems and security practices to safeguard PII.

10. US Fertility further failed to properly train its employees and monitor the computer network and systems that housed patient PII, in order to timely discover the Data Breach and implement immediate remedial measures.

11. After discovery, US Fertility also failed to timely and accurately notify Plaintiffs and Class members of the Breach.

12. As a result of Defendant's failure to implement and follow basic security procedures (including encryption, for example) and prevent the Data Breach, Plaintiffs' and other Class members' highly sensitive PII is now in the hands of thieves.

13. Plaintiffs and Class members have had to spend, and will continue to spend, significant amounts of time and money in an effort to protect themselves from the adverse ramifications of the Data Breach and will forever be at a heightened risk of identity theft and fraud.

14. 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.

15. Plaintiffs allege claims for negligence; breach of implied contract; unjust enrichment; and violations of the Maryland Personal Information Protection Act, Md. Comm. Code §§ 14-3501, *et seq.*; Maryland Consumer Protection Act, Md. Code. Ann., Cm. Law §§ 13-101, *et seq.*; and the Virginia Consumer Protection Act, Code of Virginia §§ 59.1-196, *et seq.*, and seek to compel Defendant to adopt reasonably sufficient security practices to safeguard the PII that remains in its custody in order to prevent incidents like the Data Breach from reoccurring in the future.

JURISDICTION AND VENUE

16. 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.

17. 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.

18. 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.

THE PARTIES

19. Plaintiff Nikitia Forest is a citizen of the State of Maryland and resides in Accokeek, Maryland. Plaintiff Forest sought treatment at Shady Grove Fertility, and received written notice of the Data Breach, and a true and correct copy of that Notice is attached hereto as Exhibit "A". As a result of this Data Breach, Plaintiff Forest has spent considerable time monitoring her credit report, which has caused stress and anxiety over the security of her personal information, including her credit score. As a result of her monitoring efforts, in early January 2021, Plaintiff Forest became aware that two accounts had been fraudulently opened in her name, in addition to numerous other recent credit inquiries on her account that appear to be fraudulent, including one for a car loan. Since that time, Plaintiff Forest has had to spend time handling the fraudulent accounts and further monitoring her personal accounts and information to ensure her personal information is secure. Plaintiff Forest has thus been harmed and will continue to be exposed to the risk of identity theft or some other form of fraud.

20. Plaintiff Doris Matthew is a citizen of the State of Virginia and resides in Woodbridge, Virginia. Plaintiff Matthew sought treatment at Shady Grove Fertility, and received written notice of the Data Breach, and a true and correct copy of that Notice is attached hereto as Exhibit "B". As a result of this Data Breach, Plaintiff Matthew has spent considerable time pulling and monitoring her credit report and her personal accounts and information to ensure her personal information is secure, which has caused stress and anxiety over the security of her personal information. Plaintiff Matthew has thus been harmed and

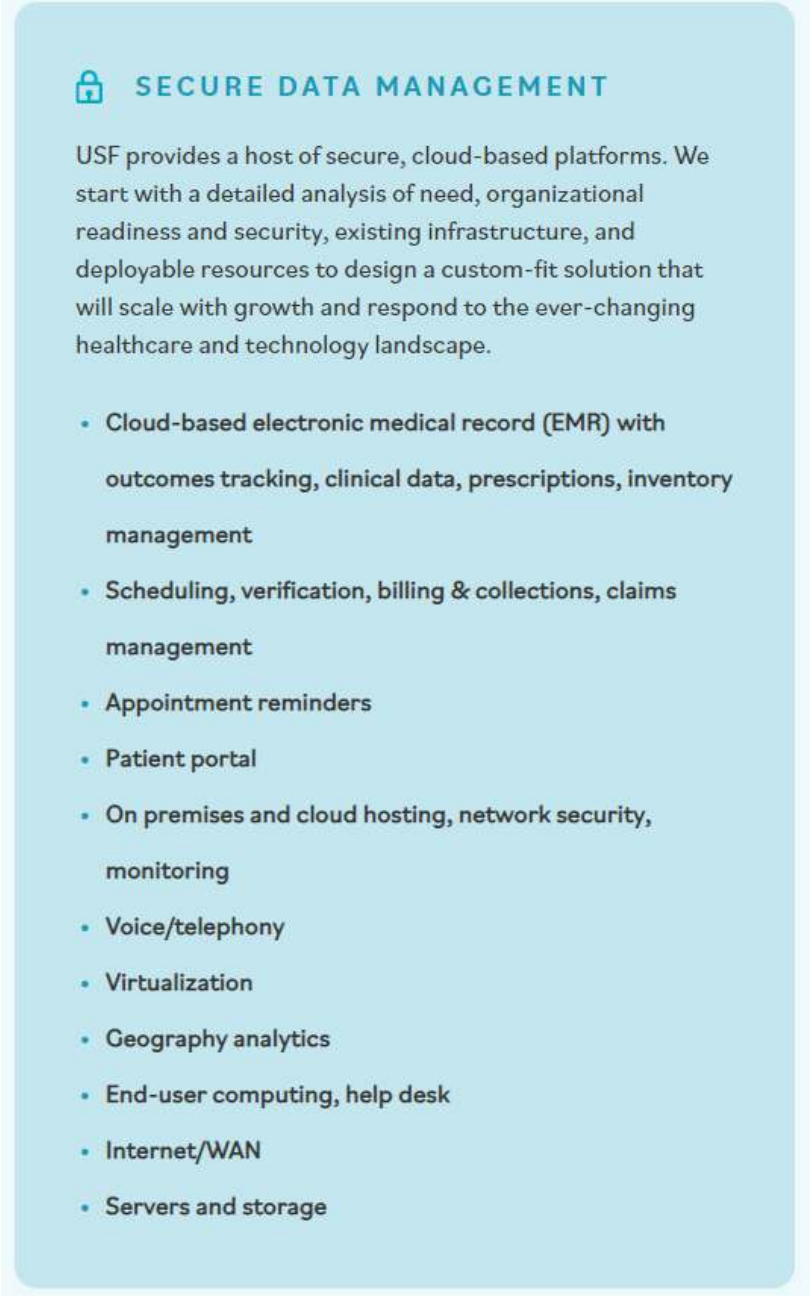
will continue to be exposed to the risk of identity theft or some other form of fraud.

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

A. The Data Breach and Defendant's Obligations to Keep PII Secure

22. US Fertility markets itself on its website as providing "Secure Data Management" with a "secure suite" of professional management services for fertility clinics:



https://www.usfertility.com/physicians/practice-success/ (last visited March 11, 2021).

23. US Fertility is also obligated by the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") to comply with a series of administrative, physical security, and technical security requirements in order to protect sensitive patient information.

24. As such, US Fertility recognizes its obligations under HIPAA to safeguard and protect patient PII. It is well known that healthcare organizations have been the target of an increasing number of cyberattacks and must take adequate and reasonable steps to protect their

systems from attack, regardless of who the intended or incidental victims are.

25. Defendant promised Plaintiffs and Class members that it would protect the privacy of their PII in accordance with federal and state laws, as well as Defendant's own privacy policies. Specifically, in a written document provided to Plaintiffs and Class members, Defendant expressly promised that it would only disclose the PII provided to it under certain circumstances, none of which relate to the Data Breach.

26. 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 PII. The PII included highly 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. The fact that patients were seeking fertility treatments makes the Data Breach even more egregious to Plaintiffs and Class members.

27. US Fertility did not begin notifying Plaintiffs and Class members until mid-November 2020, at which time it informed them that 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 US Fertility's servers.

28. The Data Breach was able to occur because Defendant 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, Defendant 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 Foreseeable and Avoidable

29. The number of U.S. data breaches have been steadily rising, and healthcare-

related data is among the most sensitive and personally consequential when compromised. The healthcare industry has thus become a prime target for hackers, and Defendant knew, or should have known, the importance of safeguarding patient PII entrusted to it and of the foreseeable consequences if its data security systems were breached, including the significant costs that would be imposed on its patients as a result of a breach. But Defendant failed to take readily available, widely known, and adequate cybersecurity measures to prevent the Data Breach from occurring.

30. Plaintiffs and Class members have taken reasonable steps to maintain the confidentiality of their PII, and they relied on US Fertility to keep their PII confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information. US Fertility 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 Breach.

31. As a result of US Fertility's conduct, Plaintiffs and Class members were, and will continue to be injured.

32. US Fertility 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.

33. Despite its awareness of its data protection obligations, US Fertility's treatment of the PII entrusted to it by Plaintiffs and Class members fell short of satisfying its legal duties and obligations. US Fertility 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

34. US Fertility was well-aware that the patient PII it collects and maintains is highly sensitive, and of significant value to those who would use it for wrongful purposes.

35. PII is a valuable commodity to identity thieves. As the FTC recognizes, identity thieves can commit an array of crimes including identify theft, medical fraud, and financial

fraud.[1] Indeed, a robust and heavily encrypted "cyber black market" exists in which criminals openly post stolen PII on multiple underground Internet websites, which are hard for law enforcement to police.

36. While credit card information can sell for as little as $1-$2 on the black market, other more sensitive information can sell for as much as $363 according to the Infosec Institute. PII is particularly valuable because criminals can use it to target victims with frauds and scams. Once PII is stolen, fraudulent use of that information and damage to victims may continue for years.

37. For example, the Social Security Administration has warned that identity thieves can use an individual's Social Security Number to apply for additional credit lines. Such fraud may go undetected until debt collection calls commence months, or even years, later. Stolen Social Security numbers also make it possible for thieves to file fraudulent tax returns, file for unemployment benefits (enabling them to collect, for example, millions of dollars in COVID-19 relief monies from state and federal governments) or apply for a job using a false identity. Each of these fraudulent activities is difficult to detect. An individual may not know that his or her Social Security Number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

38. Moreover, it is not an 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. Even then, a new Social Security number may not be effective, as "[t]he 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."[2]

---

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

[2] *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR, Brian Naylor, Feb. 9, 2015, *available at* http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft (last visited March 1, 2021).

39. This data, as one would expect, demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "[c]ompared to credit card information, personally identifiable information and Social Security numbers are worth more than 10x on the black market."[3] As explained above, the inclusion of PHI, such as the information exposed here, is even more valuable.

40. 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..."[4] In fact, the medical industry has experienced disproportionally higher instances of data theft than any other industry.

41. 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 United States in 2013," which is more "than identity thefts involving banking and finance, the government and the military, or education."[5]

42. 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."[6]

43. 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

---

[3] *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, Tim Greene, Feb. 6, 2015, *available at* http://www.itworld.com/article/2880960/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last visited March 1, 2021).

[4] Study: Few Aware of Medical Identity Theft Risk, Claims Journal, https://www.claimsjournal.com/news/national/2012/06/14/208510.htm (last visited March 11, 2021).

[5] 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 March 11, 2021).

[6] 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 March 11, 2021).

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.

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

45. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding PII and of the foreseeable consequences if its data security systems were breached, including, the significant costs that would be imposed on patients as a result of a breach.

46. There is a clear indication that the hackers who breached Defendant's systems did so not for the purpose of exacting a ransom, but for purposes of engaging in identity fraud and/or otherwise misusing the sensitive information obtained, as evidenced by the fact that Plaintiff Forest suffered a misuse of her PII immediately following the Data Breach.

D. Defendant Failed to Comply with FTC Guidelines

47. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[7]

48. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cybersecurity guidelines for businesses.[8] The guidelines note that 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

[7]Federal Trade Commission, *Start With Security*, *available at* https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last visited March 1, 2021).

[8] Federal Trade Commission, *Protecting Personal Information: A Guide for Business*, *available at* https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited March 1, 2021).

networks; understand their network's vulnerabilities; and implement policies to correct any security problems.

49. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; 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.[9]

50. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, 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 ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

51. Defendant failed to properly implement basic data security practices. Its failure to employ reasonable and appropriate measures to protect against unauthorized access to PII constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

52. Defendant was at all times fully aware of its obligation to protect the PII of patients because of its position as a healthcare provider. Defendant was also aware of the significant repercussions that would result from its failure to do so.

E. Defendant Failed to Comply with Industry Standards

53. Data exfiltrated from healthcare providers continues to be a high value target among cybercriminals, and the costs of healthcare data breaches are among the highest across all industries. As a result, both the government and private sector have developed industry best standards to address this growing problem.

54. The Department of Health and Human Services' Office for Civil Rights ("DHHS") notes that "[w]hile all organizations need to implement policies, procedures, and

[9] FTC, *Start With Security*, *supra* note 7.

technical solutions to make it harder for hackers to gain access to their systems and data, this is especially important in the healthcare industry. Hackers are actively targeting healthcare organizations as they store large quantities of highly sensitive and valuable data."[10] DHHS highlights several basic cybersecurity safeguards that can be implemented to improve cyber resilience which require a relatively small financial investment, yet can have a major impact on an organization's cybersecurity posture including: (a) the proper encryption of PII; (b) educating and training healthcare employees on how to protect PII; and (c) correcting the configuration of software and network devices.

55. Private cybersecurity firms have also identified the healthcare sector as being particularly vulnerable to cyberattacks, both because of the value of the individuals' PII they maintain and because as an industry they have been slow to adapt and respond to cybersecurity threats.[11] They too have promulgated similar best practices for bolstering cybersecurity and protecting against the unauthorized disclosure of PII.

56. Despite the abundance and availability of information regarding cybersecurity best practices for the healthcare industry, Defendant chose to ignore them. These best practices were known, or should have been known by Defendant, whose failure to heed and properly implement them directly led to the Data Breach and the unlawful exposure of Plaintiffs' and Class members' PII.

F. Plaintiffs and Class Members Have Suffered Damages

57. As a direct and proximate result of US Fertility'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,

[10] *Cybersecurity Best Practices for Healthcare Organizations*, HIPAA Journal, November 1, 2018, https://www.hipaajournal.com/important-cybersecurity-best-practices-for-healthcare-organizations/ (last visited March 1, 2021).

[11] *See, e.g.,* https://www.ntiva.com/blog/10-cybersecurity-best-practices-for-the-healthcare-industry; https://resources.infosecinstitute.com/category/healthcare-information-security/is-best-practices-for-healthcare/10-best-practices-for-healthcare-security/#gref (last visited March 1, 2021).

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.

58. 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.

59. To date, other than providing 12 months of credit monitoring and identity protection services, Defendant does not appear to be taking any measures to assist Plaintiffs and the Class members. These services are wholly inadequate as they fail to provide for the fact that victims of data breaches and other unauthorized disclosures commonly face multiple years of ongoing identity theft and financial fraud and they entirely fail to provide any compensation for the unauthorized release and disclosure of Plaintiffs' and Class members' PII.

60. Moreover, medical identity theft is not redressable through credit monitoring. Unless and until the medical bills show up through debt collection, the police show up for prescription drug abuse arrests, medical care is denied due to a non-existent condition, or life insurance or jobs are denied, a consumer is generally unaware of the violation.[12]

[12] Ponemon Institute, Fifth Annual Study on Medical Identity Theft, at 3, 12, 16 (Feb. 2015); *see also* Michelle Andrews, The Rise of Medical Identity Theft, Consumer Reports (Aug. 25, 2016); Federal Trade Commission, Medical Identity Theft, FAQs for Health Care Providers and Health

CLASS DEFINITION AND ALLEGATIONS

61. Plaintiffs bring this action on behalf of themselves and all other similarly situated consumers pursuant to Rules 23(a), (b)(2), and (b)(3) of the Federal Rules of Civil Procedure and seek certification of the following alternative Classes:

> **Nationwide Class**
> All persons residing in the United States whose PII was accessed during the Data Breach.
>
> Excluded from this Class are Defendant and its officers, directors, and employees.
>
> OR
>
> **Maryland-Only Class**
> All persons residing in Maryland whose PII was accessed during the Data Breach.
>
> Excluded from this Class are Defendant and its officers, directors, and employees.
>
> AND
>
> **Virginia-Only Class**
> All persons residing in Virginia whose PII was accessed during the Data Breach.
>
> Excluded from this Class are Defendant and its officers, directors, and employees.

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.

62. **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

---

Plans, at 1; Laura Shin, What's Behind the Dramatic Rise in Medical Identity Theft?, Fortune (Oct. 19, 2014); Identity Guard, 3 Ways Patients are at Risk for Medical Identity Theft (June 12, 2016).

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.

63. **Existence and Predominance of Common Questions of Law and Fact**. This action involves common questions of law and fact, which predominate over any questions affecting individual Class members. These common legal and factual questions include, but are not limited to, the following:

(a) Whether Defendant engaged in the wrongful conduct alleged herein;

(b) Whether Defendant's data security measures to protect Plaintiffs' and Class members' PII were reasonable;

(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 Defendant was unjustly enriched;

(h) Whether Defendant breached its implied contracts with Plaintiffs and Class members;

(i) Whether Defendant's actions violated the laws asserted;

(j) Whether Plaintiffs and Class members are entitled to appropriate remedies, including damages and other monetary relief, injunctive relief, and restitution.

64. **Typicality.** Plaintiffs' claims are typical of the claims of Class members because, *inter alia*, all Class members were subject to the Data Breach and had their PII accessed by and/or

disclosed to unauthorized third parties.

65. **Adequacy of Representation.** Plaintiffs will fairly and adequately protect the interests of Class members. Plaintiffs have retained counsel experienced in complex consumer class action litigation, and Plaintiffs intend to prosecute this action vigorously. Plaintiffs have no adverse or antagonistic interests to those of the Class members.

66. **Superiority.** A class action is superior to all other available means for the fair and efficient adjudication of this controversy. The damages or other financial detriment suffered by individual Class members is relatively small compared to the burden and expense that would be entailed by individual litigation of their claims against Defendants. It would thus be virtually impossible for Class members, on an individual basis, to obtain effective redress for the wrongs done to them. Furthermore, even if Class members could afford such individualized litigation, the court system could not. Individualized litigation would create the danger of inconsistent or contradictory judgments arising from the same set of facts. Individualized litigation would also increase the delay and expense to all parties and the court system from the issues raised by this action. By contrast, the class action device provides the benefits of adjudication of these issues in a single proceeding, economies of scale, and comprehensive supervision by a single court, and presents no unusual management difficulties under the circumstances here.

67. **Injunctive Relief.** Class certification is also appropriate under Rule 23(b)(2). Defendant, through its uniform conduct, acted or refused to act on grounds generally applicable to the Class as a whole, making injunctive and declaratory relief appropriate to the Class as a whole.

68. Unless a Class is certified, Defendant will retain monies received as a result of its conduct that was taken from Plaintiffs and Class members.

COUNT I
NEGLIGENCE

69. Plaintiffs repeat the allegations in paragraphs 1-68 as if fully set forth herein.

70. Plaintiffs bring this Count I individually and on behalf of Nationwide Class members (or, alternatively, Maryland- and Virginia-Only Class members).

71. 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.

72. 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.

73. 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.

74. Plaintiffs and Class members 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 Class members as a result of the Data Breach.

75. 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.

76. 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.

77. 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.

78. 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.

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

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

81. 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.

82. 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.

83. 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.

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

85. 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 II
BREACH OF IMPLIED CONTRACT

86. Plaintiffs repeat the allegations in paragraphs 1-68 as if fully set forth herein.

87. Plaintiffs bring this Count II individually and on behalf of the Nationwide Class members (or, alternatively, Maryland- and Virginia-Only Class members).

88. 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. Defendant promised to keep Plaintiffs' and Class members' PII secure. 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.

89. Plaintiff 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.

90. 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.

91. 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.

92. 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 III
VIOLATION OF THE MARYLAND PERSONAL INFORMATION PROTECTION ACT
Md. Comm. Law Code §§ 14-3501, *et seq.*

93. Plaintiff Forest repeats the allegations in paragraphs 1-68 as if fully set forth herein.

94. Plaintiff Forest brings this Count III individually and on behalf of the Maryland-Only Class members.

95. The Maryland Personal Information Protection Act, Md. Comm. Code §§ 14-3501, *et seq.* (the "Act") requires "a business that owns or licenses personal information of an individual residing in the State [to] implement and maintain reasonable security procedures and practices that are appropriate to the nature of personal information owned or licensed and the nature and size of the business and its operations" in order to "protect personal information from unauthorized access, use, modification, or disclosure[.]" Md. Comm. Code § 14-3503(a).

96. Defendant is a business that owns or licenses computerized data that includes personal information of individuals residing in Maryland, as defined by Md. Comm. Code §§ 14-3501(b)(1) and (2).

97. Plaintiff Forest and Class members are "individuals" and "customers" as defined and covered by Md. Comm. Code §§ 14-3502(a) and 14-3503.

98. Plaintiff's and Class members' PII includes personal information as covered under Md. Comm. Code § 14-3501(d).

99. Defendant violated the Act by failing to maintain reasonable security procedures and practices appropriate to the nature of the personal information owned or licensed and the nature and size of its business and operations.

100. The Act also requires that when a "business that owns or licenses computerized data that includes Personal Information of an individual residing in the State" discovers or is notified "of a breach of the security system" to "conduct in good faith a reasonable and prompt investigation to determine the likelihood that Personal Information of the individual has been or will be misused as a result of the breach." Md. Comm. Code § 14-3504(b)(1).

101. If, after the investigation is concluded, the business determines that the breach of the security system "creates a likelihood that personal information has been or will be misused," the Act requires that the business notify affected individuals of the breach "as soon as reasonably practicable, but not later than 45 days after" the business discovers or is notified of the breach. Md. Comm. Code §§ 14-3504(b)(2) and (c)(2).

102. The Data Breach was a "breach of the security of a system" as defined by Md. Comm. Code § 14-3504(1).

103. Defendant had notice of the Data Breach but violated the Act when it failed to disclose the Data Breach in a timely and accurate fashion.

104. As a direct and proximate result of Defendant's violations of the Act, Plaintiff and Class members suffered damages, as described above.

COUNT IV
VIOLATION OF THE MARYLAND CONSUMER PROTECTION ACT
Md. Comm. Law Code §§ 13-101, *et seq.*

105. Plaintiff Forest repeats the allegations in paragraphs 1-68 as if fully set forth herein.

106. Plaintiff Forest brings this Count III individually and on behalf of the Nationwide Class members (or, alternatively, Maryland-Only Class members).

107. As Defendant is located in, principally conducts business in, and, upon information and belief, its security systems are located in Maryland, Maryland law applies nationwide.

108. The Maryland Consumer Protection Act ("MCPA") prohibits the commission of "unfair or deceptive trade practices," and misrepresentations, which include, *inter alia*. making a "false ... or misleading oral or written statement, visual description, or other representation of any kind which has the capacity, tendency, or effect of deceiving or misleading consumers." Md. Code Ann., Com. Law § 13-301 (1).

109. Defendant engaged in unfair or deceptive trade practices and misrepresentations by, *inter alia*, misrepresenting that it had measures in place to "ensure confidentiality and integrity of data" provided to it by consumers and omitting material facts regarding the insufficiency of its data security protocols, about which it knew or should have known. Plaintiffs would not have used Defendant's services, or would have paid less for them, had they known the truth about Defendant's security practices.

110. Defendant's violation of the Maryland Personal Information Privacy Act also constitutes a violation of the MCPA, Md. Comm. Md. Code Ann., Com. Law § 14-3508.

111. Plaintiffs and Class members have been injured as a direct and proximate cause of Defendants' violations of the MCPA, as detailed above.

COUNT V
VIOLATION OF THE VIRGINIA CONSUMER PROTECTION ACT OF 1977
Code of Virginia §§ 59.1-196, *et seq.*

112. Plaintiff Matthew repeats the allegations in paragraphs 1-68 as if fully set forth herein.

113. Plaintiff Matthew brings this Count V individually and on behalf of the Virginia-Only Class members.

114. The Virginia Consumer Protection Act of 1977 ("VCPA") prohibits fraudulent acts or practices by a supplier in connection with consumer transaction. Code of Virginia § 59.1-200.

115. Defendant is a "supplier" as defined by Code of Virginia § 59.1-198.

116. Plaintiff Matthew and Virginia-Only Class members engaged in "consumer transactions" with Defendant, as defined by Code of Virginia § 59.1-198.

117. Defendant violated the VCPA by using deception, fraud, false pretense, false promise, or misrepresentation in connection with a consumer transaction when it promised consumers that their PII entrusted to it would be kept confidential and safe from unauthorized access.

118. As a result of Defendant's violation of the VCPA, Plaintiff Matthew and Virginia-Only Class members suffered losses as described above.

COUNT VI
UNJUST ENRICHMENT

119. Plaintiffs repeat the allegations in paragraphs 1-68 as if fully set forth herein.

120. Plaintiffs bring this Count VI individually and on behalf of the Nationwide Class members (or, alternatively, Maryland- and Virginia-Only Class members), and in the alternative to Count II.

121. 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.

122. 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.

123. 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.

124. 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.

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

126. 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.

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

128. 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.

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

PRAYER FOR RELIEF

Wherefore, Plaintiffs pray for a judgment:

A. Certifying the Class(es) as requested herein;

B. Appointing Plaintiffs as Class Representatives and undersigned counsel as Class Counsel;

C. Finding that Defendant engaged in the unlawful conduct 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 appropriate restitution to Plaintiffs and Class members;

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

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

I. Awarding such other and further relief as this Court may deem 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.

Dated: March 14, 2021

/s/ Tracy D. Rezvani

THE REZVANI LAW FIRM, LLC
TRACY D. REZVANI (BAR NO. 13281)
9812 Falls Road #114-291
Potomac, MD 20854-3963
Telephone: 202-350-4270
tracy@rezvanilaw.com

BONNETT, FAIRBOURN, FRIEDMAN & BALINT, P.C.
PATRICIA N. SYVERSON (*To Be Admitted Pro Hac Vice*)
600 W. Broadway, Suite 900
San Diego, California 92101
Telephone: 619-798-4593
psyverson@bffb.com

BONNETT, FAIRBOURN, FRIEDMAN & BALINT, P.C.
ELAINE A. RYAN (*To Be Admitted Pro Hac Vice*)
CARRIE A. LALIBERTE (*To Be Admitted Pro Hac Vice*)

2325 E. Camelback Rd. Suite 300
Phoenix, Arizona 85016
Telephone: 602-274-1100
eryan@bffb.com
claliberte@bffb.com

LAW OFFICE OF STAN M. DOERRER
STAN M. DOERRER (*Admission Pending*)
950 N. Washington Street
Alexandria, VA 22314
Telephone: 703-348-4646
stan@doerrerlaw.com

Attorneys for Plaintiffs and the Putative Class