UNITED STATES DISTRICT COURT
MIDDLE DISTRICT OF FLORIDA
TAMPA DIVISION

CHARLES VIVIANI, on behalf of himself and all others similarly situated, Plaintiff, v. WATSON CLINIC LLP, Defendant.	Case No.: **CLASS ACTION COMPLAINT** DEMAND FOR JURY TRIAL

Plaintiff Charles Viviani ("Plaintiff") brings this Class Action Complaint against Watson Clinic LLP ("Defendant"), individually and on behalf of all others similarly situated ("Class Members"), and alleges, upon personal knowledge as to his own actions and his counsels' investigations, and upon information and belief as to all other matters, as follows:

I. INTRODUCTION

1. Plaintiff brings this class action against Defendant for its failure to properly secure and safeguard personal identifiable information ("PII")[1] of Defendant's current and former patients, including name, address, birthdate, Social Security number or similar government identifier, driver's license number, financial

[1] Personally identifiable information generally incorporates information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information. 2 C.F.R. § 200.79. At a minimum, it includes all information that on its face expressly identifies an individual.

account information, and/or medical information, which may include details such as diagnoses, treatments, or medical record numbers.

2. According to its website, Defendant has "a total staff of more than 1600 team members, over 350 physicians and providers, 40 diverse medical and surgical specialties and 19 state-of-the-art locations welcoming well over a million outpatient visits every year."

3. Defendant's Notice of Privacy Practices states, under "Our Responsibilities," as follows:

- We are required by law to maintain the privacy and security of your protected health information.
- We try to keep your data secure, but we cannot guarantee that nothing will go wrong. We will let you know promptly if a breach occurs that may have compromised the privacy or security of your information.

4. Prior to and through February 6, 2024, Defendant obtained the PII of Plaintiff and Class Members and stored that PII, unencrypted, in an Internet-accessible environment on Defendant's network.

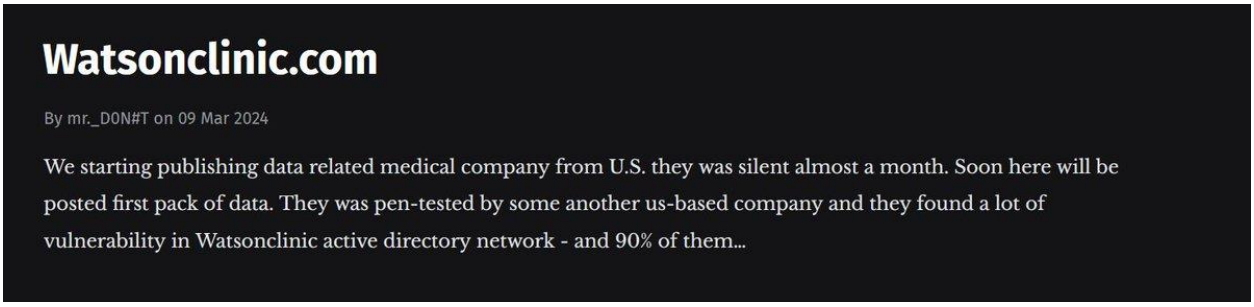
5. On or around February 6, 2024, Defendant discovered that an unauthorized third party gained access to a limited portion of its network starting on January 26, 2024 (the "Data Breach").

6. Defendant determined that the unauthorized actor may have accessed

the PII of Plaintiff and Class Members.

7. On or around March 9, 2024, reports began surfacing on the Internet that Defendant had been the subject of a ransomware attack by the DonutLeaks ransomware group.

8. On or about March 9, 2024, the DonutLeaks ransomware group stated that it was publishing information exfiltrated during the data breach due to Defendant's silence over the previous month, presumably regarding a ransom demand, as follows:



9. On or around March 9, 2024, the DonutLeaks ransomware group posted a screenshot showing it had accessed Defendant's systems.

10. On or around April 26, 2024, Defendant posted a Notice of Data Security Incident on its website regarding the Data Breach, which did not disclose that the DonutLeaks ransomware group had claimed responsibility for the Data Breach and had stated its intent to publish information exfiltrated during the Data Breach.

11. On or around August 26, 2024, Defendant posted an Updated Notice of

Data Security Incident on its website, which did not disclose that the DonutLeaks ransomware group had claimed responsibility for the Data Breach and had stated its intent to publish information exfiltrated during the Data Breach.

12. On or around August 26, 2024, Defendant began notifying various state Attorneys General of the Data Breach.

13. On or around August 26, 2024, Defendant began notifying Plaintiff and Class Members of the Data Breach via mail.

14. The notices that Defendant sent to Plaintiff and Class Members did not disclose that did not disclose that the DonutLeaks ransomware group had claimed responsibility for the Data Breach and had stated its intent to publish information exfiltrated during the Data Breach.

15. By obtaining, collecting, using, and deriving a benefit from the PII of Plaintiff and Class Members, Defendant assumed legal and equitable duties to those individuals to protect and safeguard that information from unauthorized access and intrusion. Defendant admits that the exfiltrated information included name, address, birthdate, Social Security number or similar government identifier, driver's license number, financial account information, and/or medical information, which may include details such as diagnoses, treatments, or medical record numbers.

16. The exposed PII of Plaintiff and Class Members can be sold on the dark web. Hackers can access and then offer for sale the unencrypted, unredacted PII to

criminals. Plaintiff and Class Members now face a lifetime risk of (i) identity theft, which is heightened here by the loss of Social Security numbers, and (ii) the sharing and detrimental use of their confidential medical information.

17. The PII were compromised due to Defendant's negligent and/or careless acts and omissions and the failure to protect the PII of Plaintiff and Class Members. In addition to Defendant's failure to prevent the Data Breach, Defendant waited several months after the Data Breach occurred to report it to the states' Attorneys General and affected individuals. Defendant has also purposefully maintained secret the specific vulnerabilities and root causes of the breach and has not informed Plaintiff and Class Members of that information.

18. As a result of this delayed response, Plaintiff and Class Members had no idea their PII had been compromised, and that they were, and continue to be, at significant risk of identity theft and various other forms of personal, social, and financial harm, including the sharing and detrimental use of their confidential medical information. The risk will remain for their respective lifetimes.

19. Plaintiff brings this action on behalf of all persons whose PII was compromised as a result of Defendant's failure to: (i) adequately protect the PII of Plaintiff and Class Members; (ii) warn Plaintiff and Class Members of Defendant's inadequate information security practices; and (iii) effectively secure hardware containing protected PII using reasonable and effective security procedures free of

vulnerabilities and incidents. Defendant's conduct amounts to negligence and violates federal and state statutes.

20. Plaintiff and Class Members have suffered injury as a result of Defendant's conduct. These injuries include: (i) lost or diminished value of PII; (ii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (iii) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time, (iv) the disclosure of their private information, including medical information, and (v) the continued and certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) may remain backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fail to undertake appropriate and adequate measures to protect the PII.

21. Defendant disregarded the rights of Plaintiff and Class Members by intentionally, willfully, recklessly, or negligently failing to take and implement adequate and reasonable measures to ensure that the PII of Plaintiff and Class Members was safeguarded, failing to take available steps to prevent an unauthorized disclosure of data, and failing to follow applicable, required and appropriate protocols, policies and procedures regarding the encryption of data, even for internal use. As the result, the PII of Plaintiff and Class Members was compromised through

disclosure to an unknown and unauthorized third party. Plaintiff and Class Members have a continuing interest in ensuring that their information is and remains safe, and they should be entitled to injunctive and other equitable relief.

II. PARTIES

22. Plaintiff is a Citizen of Florida residing in Plant City, Florida.

23. Defendant is a corporation organized under the laws of Florida with a principal place of business in Lakeland, Florida.

24. The true names and capacities of persons or entities, whether individual, corporate, associate, or otherwise, who may be responsible for some of the claims alleged herein are currently unknown to Plaintiff. Plaintiff will seek leave of court to amend this complaint to reflect the true names and capacities of such other responsible parties when their identities become known.

25. All of Plaintiff's claims stated herein are asserted against Defendant and any of its owners, predecessors, successors, subsidiaries, agents and/or assigns.

III. JURISDICTION AND VENUE

26. This Court has subject matter and diversity jurisdiction over this action under 28 U.S.C. § 1332(d) because this is a class action wherein the amount of controversy exceeds the sum or value of $5 million, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one Class

Member is a citizen of a state different from Defendant to establish minimal diversity.

27. Defendant is a citizen of Florida because it is a corporation formed under Florida law with its principal place of business in Lakeland, Florida.

28. The Middle District of Florida has personal jurisdiction over Defendant because it conducts substantial business in Florida and this District and collected and/or stored the PII of Plaintiff and Class Members in this District.

29. Venue is proper in this District under 28 U.S.C. §1391(b) because Defendant operates in this District and a substantial part of the events or omissions giving rise to Plaintiffs' claims occurred in this District, including Defendant collecting and/or storing the PII of Plaintiff and Class Members.

IV. FACTUAL ALLEGATIONS

Background

30. Plaintiff and Class Members, who obtained services from Defendant, provided and entrusted Defendant with sensitive and confidential information, including name, address, birthdate, Social Security number or similar government identifier, driver's license number, financial account information, and/or medical information, which may include details such as diagnoses, treatments, or medical record numbers.

31. Plaintiff and Class Members relied on these sophisticated Defendant 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. Plaintiff and Class Members demand security to safeguard their PII.

32. Defendant had a duty to adopt reasonable measures to protect the PII of Plaintiff and Class Members from involuntary disclosure to third parties.

The Data Breach

33. On or about August 26, 2024, Defendant sent Plaintiff and Class Members a notice of the Data Breach (the "Notice of Security Event"). Defendant informed Plaintiff and other Class Members that:

> Watson Clinic is writing to inform you of an incident involving potential unauthorized access to your information. Earlier this year, we detected a cybersecurity incident involving unauthorized activity in portions of our computer network. We promptly began investigating. Based on the investigation, we determined that the unauthorized third party may have acquired some of your personal information and/or protected health information. We are providing this notice to give you more information on what happened and what we are doing in response.
>
> **WHAT HAPPENED**
> An unauthorized third party gained access to portions of our network starting on January 26, 2024, and we discovered the intrusion on February 6, 2024. We promptly began investigating, engaged third-party cybersecurity experts through outside counsel, and started remediation efforts, including identifying the potentially affected files and engaging a data-review firm to analyze their contents. We received those results in early July 2024 and have been working since that time to compile contact information for notifying impacted individuals.

> **WHAT INFORMATION WAS INVOLVED** We have not been able to confirm whether the unauthorized third party actually viewed or acquired the files containing your personal information or protected health information. But, because the unauthorized third party potentially accessed those files, we are providing this notice out of an abundance of caution. We determined that the unauthorized third party potentially accessed some of your personal information and protected health information, . The unauthorized third party also potentially accessed some of your medical information, which may include details such as diagnoses, treatments, or medical record numbers.

34. Defendant admitted in the Notice of Security Event and the notices posted on its website that an unauthorized actor potentially accessed data about patients, including name, address, birthdate, Social Security number or similar government identifier, driver's license number, financial account information, and/or medical information, which may include details such as diagnoses, treatments, or medical record numbers.

35. In response to the Data Breach, Defendant claims that it "hired third-party experts to help us address this situation, perform an investigation into the unauthorized activity, and further secure our systems and the information we maintain as we move forward."

36. However, the details of the root cause of the Data Breach, the vulnerabilities exploited, and the remedial measures undertaken to ensure a breach does not occur again have not been shared with regulators or Plaintiff and Class

Members, who retain a vested interest in ensuring that their information remains protected.

37. The unencrypted PII of Plaintiff and Class Members may end up for sale on the dark web, or simply fall into the hands of companies that will use the detailed PII for targeted marketing without the approval of Plaintiff and Class Members. Unauthorized individuals can easily access the PII of Plaintiff and Class Members.

38. Defendant did not use reasonable security procedures and practices appropriate to the nature of the sensitive, unencrypted information it was maintaining for Plaintiff and Class Members, causing the exposure of PII for Plaintiff and Class Members.

39. Because Defendant had a duty to protect Plaintiff's and Class Members' PII, Defendant should have accessed readily available and accessible information about potential threats for the unauthorized exfiltration and misuse of such information.

40. In the years immediately preceding the Data Breach, Defendant knew or should have known that Defendant's computer systems were a target for cybersecurity attacks, including ransomware attacks involving data theft, because warnings were readily available and accessible via the internet.

41. In October 2019, the Federal Bureau of Investigation published online

an article titled "High-Impact Ransomware Attacks Threaten U.S. Businesses and Organizations" that, among other things, warned that "[a]lthough state and local governments have been particularly visible targets for ransomware attacks, ***ransomware actors have also targeted health care organizations***, ***industrial companies***, and the transportation sector."[2]

42. In April 2020, ZDNet reported, in an article titled "Ransomware mentioned in 1,000+ SEC filings over the past year," that "***[r]ansomware gangs are now ferociously aggressive in their pursuit of big companies***. They breach networks, use specialized tools to maximize damage, ***leak corporate information on dark web portals***, and even tip journalists to generate negative news for companies as revenge against those who refuse to pay."[3]

43. In September 2020, the United States Cybersecurity and Infrastructure Security Agency published online a "Ransomware Guide" advising that ***"[m]alicious actors have adjusted their ransomware tactics over time to include pressuring victims for payment by threatening to release stolen data*** if they refuse

[2] FBI, High-Impact Ransomware Attacks Threaten U.S. Businesses and Organizations (Oct. 2, 2019) (emphasis added), *available at* https://www.ic3.gov/Media/Y2019/PSA191002 (last visited Jan. 25, 2022).

[3] ZDNet, Ransomware mentioned in 1,000+ SEC filings over the past year (Apr. 30, 2020) (emphasis added), *available at* https://www.zdnet.com/article/ransomware-mentioned-in-1000-sec-filings-over-the-past-year/ (last visited Jan. 25, 2022).

to pay and publicly naming and shaming victims as secondary forms of extortion."[4]

44. This readily available and accessible information confirms that, prior to the Data Breach, Defendant knew or should have known that (i) ransomware actors were targeting healthcare companies such as Defendant, (ii) ransomware gangs were ferociously aggressive in their pursuit of big companies such as Defendant, (iii) ransomware gangs were leaking corporate information on dark web portals, and (iv) ransomware tactics included threatening to release stolen data.

45. In light of the information readily available and accessible on the internet before the Data Breach, Defendant, having elected to store the unencrypted PII of Plaintiff and Class Members in an Internet-accessible environment, had reason to be on guard for the exfiltration of the PII and Defendant's type of business had cause to be particularly on guard against such an attack.

46. Prior to the Data Breach, Defendant knew or should have known that there was a foreseeable risk that Plaintiff's and Class Members' PII could be accessed, exfiltrated, and published as the result of a cyberattack.

47. Prior to the Data Breach, Defendant knew or should have known that it should have encrypted the Social Security numbers and other sensitive data elements within the PII to protect against their publication and misuse in the event of a

[4] U.S. CISA, Ransomware Guide – September 2020, *available at* https://www.cisa.gov/sites/default/files/publications/CISA_MS ISAC_Ransomware%20Guide_S508C_.pdf (last visited Jan. 25, 2022).

cyberattack.

Defendant Acquires, Collects, and Stores the PII of Plaintiff and Class Members.

48. As a condition of obtaining services from Defendant, Defendant required that Plaintiff and Class Members entrust Defendant with highly confidential PII.

49. Defendant acquired, collected, and stored the PII of Plaintiff and Class Members.

50. By obtaining, collecting, and storing the PII of Plaintiff and Class Members, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting the PII from disclosure.

51. Plaintiff and Class Members have taken reasonable steps to maintain the confidentiality of their PII and relied on Defendant 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.

Securing PII and Preventing Breaches

52. Defendant could have prevented this Data Breach by properly securing and encrypting the folders, files, and or data fields containing the PII of Plaintiff and Class Members. Alternatively, Defendant could have destroyed the data it no longer had a reasonable business need to maintain or only stored data in an Internet-accessible environment when there was a reasonable need to do so.

53. Defendant's negligence in safeguarding the PII of Plaintiff and Class Members is exacerbated by the repeated warnings and alerts directed to protecting and securing sensitive data.

54. Despite the prevalence of public announcements of data breach and data security compromises, Defendant failed to take appropriate steps to protect the PII of Plaintiff and Class Members from being compromised.

55. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[5] The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."[6]

56. The ramifications of Defendant's failure to keep secure the PII of Plaintiff and Class Members are long lasting and severe. Once PII is stolen, particularly Social Security numbers, fraudulent use of that information and damage to victims may continue for years.

[5] 17 C.F.R. § 248.201 (2013).

[6] *Id.*

Value of Personal Identifiable Information

57. The PII of individuals 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, and bank details have a price range of $50 to $200.[7] Experian reports that a stolen credit or debit card number can sell for $5 to $110 on the dark web.[8] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[9]

58. Social Security numbers, for example, 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:

> 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.

[7] *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. 26, 2022).

[8] *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, *available at*: https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last accessed Jan. 26, 2022).

[9] *In the Dark*, VPNOverview, 2019, *available at*: https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last accessed Dec. 29, 2020).

> 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.[10]

59. What is 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.

60. 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."[11]

61. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card

---

[10] Social Security Administration, *Identity Theft and Your Social Security Number*, *available at*: https://www.ssa.gov/pubs/EN-05-10064.pdf (last accessed Jan. 26, 2022).

[11] 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 accessed Jan. 26, 2022).

information in a retailer data breach because, there, victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change—Social Security number, driver's license or state identification number, and biometrics.

62. This data demands 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 10x on the black market."[12]

63. Among other forms of fraud, identity thieves may obtain driver's licenses, government benefits, medical services, and housing or even give false information to police.

64. The fraudulent activity resulting from the Data Breach may not come to light for years.

65. There may be a time lag between when harm occurs versus when it is discovered, and also between when PII is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases,

[12] 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 accessed Jan. 26, 2022).

> stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[13]

66. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the PII of Plaintiff and Class Members, including Social Security numbers, and of the foreseeable consequences that would occur if Defendant's data security system was breached, including, specifically, the significant costs that would be imposed on Plaintiff and Class Members as a result of a breach.

67. Plaintiff and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their PII.

68. Defendant was, or should have been, fully aware of the unique type and the significant volume of data contained in Defendant's folders and files, amounting to potentially thousands of individuals' detailed, personal information and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

---

[13] *Report to Congressional Requesters*, GAO, at 29 (June 2007), *available at:* https://www.gao.gov/assets/gao-07-737.pdf (last accessed Mar. 15, 2021).

69. To date, Defendant has offered Plaintiff and Class Members 1 year of credit monitoring and identity protection services.

70. The injuries to Plaintiff and Class Members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for the PII of Plaintiff and Class Members.

Plaintiff's Experience

71. Plaintiff's services from Defendant ended more than ten (10) years prior to the Data Breach. As a condition of providing services to Plaintiff, Defendant required that he provide and entrust his PII.

72. Plaintiff received Defendant's Notice of Data Security Event, dated August 26, 2024, on or about that date. The notice stated that Plaintiff's name, contact information, birthdate, Social Security number or similar government identifier, and medical information, including diagnoses, treatments, or medical record numbers, were potentially accessed during the Data Breach. Reports on the Internet indicate that the PII was actually exfiltrated and posted on the dark web.

73. As a result of the Data Breach, Plaintiff's PII was exfiltrated by an unauthorized actor. The confidentiality of Plaintiff's PII has been irreparably harmed. For the rest of his life, Plaintiff will have to worry about when and how his PII may be shared or used to his detriment.

74. As a result of the Data Breach notice, Plaintiff spent time dealing with

the consequences of the Data Breach, which includes time spent verifying the legitimacy of the Important Security Notification. This time has been lost forever and cannot be recaptured.

75. Additionally, Plaintiff is very careful about sharing his sensitive PII. He has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source.

76. Plaintiff stores any documents containing his sensitive PII in a safe and secure location or destroys the documents. Moreover, he diligently chooses unique usernames and passwords for his various online accounts.

77. Plaintiff suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of his privacy.

78. Plaintiff has suffered imminent and impending injury arising from the substantially increased risk misuse resulting from his PII being placed in the hands of unauthorized third parties and possibly criminals.

79. Plaintiff has a continuing interest in ensuring that his PII, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

V. CLASS ALLEGATIONS

80. Plaintiff brings this nationwide class action on behalf of himself and on

behalf of all others similarly situated pursuant to Rule 1.220(b)(2), (b)(3), and (d)(4) of the Florida Rules of Civil Procedure.

81. The Nationwide Class that Plaintiff seeks to represent is defined as follows:

> All individuals whose PII was obtained or potentially obtained in the data breach that is the subject of the notice that Defendant sent to Plaintiff and Class Members on or around August 26, 2024 (the "Nationwide Class").

82. Excluded from the Class are the following individuals and/or entities: Defendant and Defendant's parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendant has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; any and all federal, state or local governments, including but not limited to their departments, agencies, divisions, bureaus, boards, sections, groups, counsels and/or subdivisions; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

83. Plaintiff reserves the right to modify or amend the definition of the proposed classes before the Court determines whether certification is appropriate.

84. Numerosity, Fla R. Civ. P. 1.220(a)(1): The Classes are so numerous that joinder of all members is impracticable. Defendant, which is based in Florida, reported that 194 New Hampshire residents were impacted.

85. Commonality, Fla. R. Civ. P. 1.220(a)(2) and (b)(3): Questions of law

and fact common to the Classes exist and predominate over any questions affecting only individual Class Members. These include:

a. Whether and to what extent Defendant had a duty to protect the PII of Plaintiff and Class Members;

b. Whether Defendant had duties not to disclose the PII of Plaintiff and Class Members to unauthorized third parties;

c. Whether Defendant had duties not to use the PII of Plaintiff and Class Members for non-business purposes;

d. Whether Defendant failed to adequately safeguard the PII of Plaintiff and Class Members;

e. When Defendant actually learned of the Data Breach;

f. Whether Defendant adequately, promptly, and accurately informed Plaintiff and Class Members that their PII had been compromised;

g. Whether Defendant violated the law by failing to promptly notify Plaintiff and Class Members that their PII had been compromised;

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

i. Whether Defendant adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

j. Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard the PII of Plaintiff and Class Members;

k. Whether Plaintiff and Class Members are entitled to actual, consequential, and/or nominal damages as a result of Defendant's wrongful conduct;

l. Whether Plaintiff and Class Members are entitled to restitution as a result of Defendant's wrongful conduct; and

m. Whether Plaintiff and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach.

86. Typicality, Fla. R. Civ. P. 1.220(a)(3): Plaintiff's claims are typical of those of other Class Members because all had their PII compromised as a result of the Data Breach, due to Defendant's misfeasance.

87. Policies Generally Applicable to the Classes: This class action is also appropriate for certification because Defendant has acted or refused to act on grounds generally applicable to the Classes, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward Class Members and making final injunctive relief appropriate with respect to the Classes as a whole. Defendant's policies challenged herein apply to and affect Class Members uniformly and Plaintiff's challenge of these policies hinges on Defendant's conduct with

respect to the Classes as a whole, not on facts or law applicable only to Plaintiff.

88. Adequacy, Fla R. Civ. P. 1.220(a)(4): Plaintiff will fairly and adequately represent and protect the interests of Class Members in that he has no disabling conflicts of interest that would be antagonistic to those of the other Members of the Classes. Plaintiff seeks no relief that is antagonistic or adverse to the Members of the Classes and the infringement of the rights and the damages he has suffered are typical of other Class Members. Plaintiff has retained counsel experienced in complex class action litigation, and Plaintiff intends to prosecute this action vigorously.

89. Superiority and Manageability, Fla R. Civ. P. 1.220(b)(3): The class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of Class Members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain Class Members, who could not individually afford to litigate a complex claim against large corporations, like Defendant. Further, even for those Class Members who could afford to litigate such a claim, it would still be economically impractical and impose

a burden on the courts.

90. The nature of this action and the nature of laws available to Plaintiff and Class Members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiff and Class Members for the wrongs alleged because Defendant would necessarily gain an unconscionable advantage since it would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiff was exposed is representative of that experienced by the Classes and will establish the right of each Class Member to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

91. The litigation of the claims brought herein is manageable. Defendant's uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrates that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

92. Adequate notice can be given to Class Members directly using information maintained in Defendant's records.

93. Unless a Class-wide injunction is issued, Defendant may continue in its

failure to properly secure the PII of Class Members, Defendant may continue to refuse to provide proper notification to Class Members regarding the Data Breach, and Defendant may continue to act unlawfully as set forth in this Complaint.

94. Further, Defendant has acted or refused to act on grounds generally applicable to the Classes and, accordingly, final injunctive or corresponding declaratory relief with regard to Class Members as a whole is appropriate under Rule 1.220(b)(2) of the Florida Rules of Civil Procedure.

95. Likewise, particular issues under Rule 1.220(d)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendant owed a legal duty to Plaintiff and Class Members to exercise due care in collecting, storing, using, and safeguarding their PII;

b. Whether Defendant breached a legal duty to Plaintiff and Class Members to exercise due care in collecting, storing, using, and safeguarding their PII;

c. Whether Defendant failed to comply with its own policies and applicable laws, regulations, and industry standards relating to data security;

d. Whether an implied contract existed between Defendant on the one hand, and Plaintiff and Class Members on the other, and the terms of that implied contract;

e. Whether Defendant breached the implied contract;

f. Whether Defendant adequately and accurately informed Plaintiff and Class Members that their PII had been compromised;

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

h. Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard the PII of Plaintiff and Class Members; and,

i. Whether Class Members are entitled to actual, consequential, and/or nominal damages, and/or injunctive relief as a result of Defendant's wrongful conduct.

COUNT I
NEGLIGENCE
(On Behalf of Plaintiff and the Nationwide Class)

96. Plaintiff and the Nationwide Class re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 95.

97. As a condition of obtaining services from Defendant, Plaintiff and Class

Members were obligated to provide and entrust Defendant with certain PII.

98. Plaintiff and the Nationwide Class provided and entrusted their PII to Defendant on the premise and with the understanding that Defendant would safeguard their information, use their PII for business purposes only, and not disclose their PII to unauthorized third parties.

99. Defendant has full knowledge of the sensitivity of the PII and the types of harm that Plaintiff and the Nationwide Class could and would suffer if the PII were wrongfully disclosed.

100. Defendant knew or reasonably should have known that the failure to exercise due care in the collecting, storing, and using of the PII of Plaintiff and the Nationwide Class involved an unreasonable risk of harm to Plaintiff and the Nationwide Class, even if the harm occurred through the criminal acts of a third party.

101. Defendant had a duty to exercise reasonable care in safeguarding, securing, and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties. This duty includes, among other things, designing, maintaining, and testing Defendant's security protocols to ensure that the PII of Plaintiff and the Nationwide Class in Defendant's possession was adequately secured and protected.

102. Defendant also had a duty to exercise appropriate clearinghouse

practices to remove from an Internet-accessible environment the PII it was no longer required to retain pursuant to regulations and had no reasonable business need to maintain in an Internet-accessible environment.

103. Defendant also had a duty to have procedures in place to detect and prevent the improper access and misuse of the PII of Plaintiff and the Nationwide Class.

104. Defendant's duty to use reasonable security measures arose as a result of the special relationship that existed between Defendant and Plaintiff and the Nationwide Class. That special relationship arose because Plaintiff and the Nationwide Class entrusted Defendant with their confidential PII, a necessary part of obtaining services from Defendant.

105. Defendant was subject to an "independent duty," untethered to any contract between Defendant and Plaintiff or the Nationwide Class.

106. A breach of security, unauthorized access, and resulting injury to Plaintiff and the Nationwide Class was reasonably foreseeable, particularly in light of Defendant's inadequate security practices.

107. Plaintiff and the Nationwide Class were the foreseeable and probable victims of any inadequate security practices and procedures. Defendant knew or should have known of the inherent risks in collecting and storing the PII of Plaintiff and the Nationwide Class, the critical importance of providing adequate security of

that PII, and the necessity for encrypting PII stored on Defendant's systems.

108. Defendant's own conduct created a foreseeable risk of harm to Plaintiff and the Nationwide Class. Defendant's misconduct included, but was not limited to, their failure to take the steps and opportunities to prevent the Data Breach as set forth herein. Defendant's misconduct also included their decisions not to comply with industry standards for the safekeeping of the PII of Plaintiff and the Nationwide Class, including basic encryption techniques freely available to Defendant.

109. Plaintiff and the Nationwide Class had no ability to protect their PII that was in, and possibly remains in, Defendant's possession.

110. Defendant was in a position to protect against the harm suffered by Plaintiff and the Nationwide Class as a result of the Data Breach.

111. Defendant had and continue to have a duty to adequately disclose that the PII of Plaintiff and the Nationwide Class within Defendant's possession might have been compromised, how it was compromised, and precisely the types of data that were compromised and when. Such notice was necessary to allow Plaintiff and the Nationwide Class to (i) take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their PII by third parties and (ii) prepare for the sharing and detrimental use of their confidential medical information.

112. Defendant had a duty to employ proper procedures to prevent the unauthorized dissemination of the PII of Plaintiff and the Nationwide Class.

113. Defendant has admitted that the PII of Plaintiff and the Nationwide Class was wrongfully lost and disclosed to unauthorized third persons as a result of the Data Breach.

114. Defendant, through its actions and/or omissions, unlawfully breached their duties to Plaintiff and the Nationwide Class by failing to implement industry protocols and exercise reasonable care in protecting and safeguarding the PII of Plaintiff and the Nationwide Class during the time the PII was within Defendant's possession or control.

115. Defendant improperly and inadequately safeguarded the PII of Plaintiff and the Nationwide Class in deviation of standard industry rules, regulations, and practices at the time of the Data Breach.

116. Defendant failed to heed industry warnings and alerts to provide adequate safeguards to protect the PII of Plaintiff and the Nationwide Class in the face of increased risk of theft.

117. Defendant, through its actions and/or omissions, unlawfully breached their duty to Plaintiff and the Nationwide Class by failing to have appropriate procedures in place to detect and prevent dissemination of the PII.

118. Defendant breached its duty to exercise appropriate clearinghouse practices by failing to remove from the Internet-accessible environment any PII it was no longer required to retain pursuant to regulations and which Defendant had

no reasonable need to maintain in an Internet-accessible environment.

119. Defendant, through its actions and/or omissions, unlawfully breached their duty to adequately and timely disclose to Plaintiff and the Nationwide Class the existence and scope of the Data Breach.

120. But for Defendant's wrongful and negligent breach of duties owed to Plaintiff and the Nationwide Class, the PII of Plaintiff and the Nationwide Class would not have been compromised.

121. There is a close causal connection between Defendant's failure to implement security measures to protect the PII of Plaintiff and the Nationwide Class and the harm, or risk of imminent harm, suffered by Plaintiff and the Nationwide Class. The PII of Plaintiff and the Nationwide Class was exfiltrated as the proximate result of Defendant's failure to exercise reasonable care in safeguarding such PII by adopting, implementing, and maintaining appropriate security measures.

122. As a direct and proximate result of Defendant's negligence, Plaintiff and the Nationwide Class have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity of how their PII is used; (iii) the compromise, 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) the continued risk to their PII, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII of Plaintiff and the Nationwide Class; and (viii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and the Nationwide Class.

123. As a direct and proximate result of Defendant's negligence, Plaintiff and the Nationwide Class have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

124. Additionally, as a direct and proximate result of Defendant's negligence, Plaintiff and the Nationwide Class have suffered and will suffer the continued risks of exposure of their PII, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII in its continued possession.

125. As a direct and proximate result of Defendant's negligence, Plaintiff and the Nationwide Class are entitled to recover actual, consequential, and nominal damages.

COUNT II
BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiff and the Nationwide Class)

126. Plaintiff re-alleges and incorporate by reference herein all of the allegations contained in paragraphs 1 through 95.

127. In obtaining services from Defendant, Plaintiff and Nationwide Class Members provided and entrusted their PII to Defendant.

128. Defendant required Plaintiff and Nationwide Class Members to provide and entrust their PII as a condition of obtaining services from Defendant.

129. As a condition of obtaining services from Defendant, Plaintiff and Nationwide Class Members provided and entrusted their PII. In so doing, Plaintiff and Nationwide Class Members entered into implied contracts with Defendant by which Defendant agreed to safeguard and protect such PII, to keep such PII secure and confidential, and to timely and accurately notify Plaintiff and Nationwide Class Members if their PII had been compromised or stolen.

130. In its Notice of Privacy Practices, Defendant stated that it (i) is "required by law to maintain the privacy and security of [patients'] protected health information" and (ii) "tr[ies] to keep [patient] data secure."

131. Plaintiff and the Nationwide Class Members fully performed their obligations under the implied contracts with Defendant.

132. Defendant breached the implied contracts it made with Plaintiff and Nationwide Class Members by failing to comply with laws requiring it to maintain the privacy and security of patients' protected health information, including Fla. Stat. § 456.057; failing to try to keep patient data secure, including by failing to encrypt patient Social Security numbers and other sensitive PII while storing it in an Internet-accessible environment and failing to purge the PII of former patients absent a reasonable need to store it in an Internet-accessible environment; and otherwise failing to safeguard and protect patient PII.

133. As a direct and proximate result of Defendant's above-described breach of implied contract, Plaintiff and Nationwide Class Members have suffered (and will continue to suffer) the threat of the sharing and detrimental use of their confidential medical information; ongoing, imminent, and impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; loss of the confidentiality of the stolen confidential data; the illegal sale of the compromised data on the dark web; expenses and/or time spent on credit monitoring and identity theft insurance; time spent scrutinizing bank statements, credit card statements, and credit reports; expenses and/or time spent initiating fraud alerts,

decreased credit scores and ratings; lost work time; and other economic and non-economic harm.

134. As a direct and proximate result of Defendant's above-described breach of implied contract, Plaintiff and Nationwide Class Members are entitled to recover actual, consequential, and nominal damages.

COUNT III
BREACH OF FIDUCIARY DUTY
(On Behalf of Plaintiff and the Nationwide Class)

135. Plaintiff re-alleges and incorporate by reference herein all of the allegations contained in paragraphs 1 through 95.

136. A relationship existed between Plaintiff and the Nationwide Class and Defendant in which Plaintiff and the Nationwide Class put their trust in Defendant to protect the private information of Plaintiff and the Nationwide Class and Defendant accepted that trust.

137. Fla. Stat. § 456.057(10) provides that "All records owners shall develop and implement policies, standards, and procedures to protect the confidentiality and security of the medical record. Employees of records owners shall be trained in these policies, standards, and procedures." A "record owner" includes "any health care practitioner who generates a medical record after making a physical or mental examination of, or administering treatment or dispensing legend drugs to, any person." Fla. Stat. § 456.057(1).

138. "[T]he requirement of doctor-patient confidentiality" prescribed in Section 456.057 "creates 'a relation of trust and confidence ... between the parties' giving rise to a fiduciary duty, the breach of which is actionable in tort." *LeBlanc v. Acevedo*, 258 So. 3d 555, 558 (Fla. 5th DCA 2018) (quoting *Gracey v. Eaker*, 837 So.2d 348, 352 (Fla. 2002)).

139. Defendant breached the fiduciary duty that it owed to Plaintiff and the Nationwide Class by failing to act with the utmost good faith, fairness, and honesty, failing to act with the highest and finest loyalty, and failing to protect the private information of Plaintiff and the Nationwide Class.

140. Defendant's breach of fiduciary duty was a legal cause of damage to Plaintiff and the Nationwide Class.

141. But for Defendant's breach of fiduciary duty, the damage to Plaintiff and the Nationwide Class would not have occurred.

142. Defendant's breach of fiduciary duty contributed substantially to producing the damage to Plaintiff and the Nationwide Class.

143. As a direct and proximate result of Defendant's breach of fiduciary duty, Plaintiff and the Nationwide Class are entitled to and demand actual, consequential, and nominal damages and injunctive relief.

COUNT IV
VIOLATION OF THE FLORIDA DECEPTIVE AND UNFAIR TRADE PRACTICES ACT,
Fla. Stat. § 501.201, *et seq.* ("FDUTPA")
(On Behalf of Plaintiff and the Nationwide Class and Against Defendant)

144. Plaintiff and the Nationwide Class re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 95.

145. This cause of action is brought pursuant the FDUTPA, which, pursuant to Fla. Stat. § 501.202, requires such claims be "construed liberally" by the courts "[t]o protect the consuming public and legitimate business enterprises from those who engage in unfair methods of competition, or unconscionable, deceptive, or unfair acts or practices in the conduct of any trade or commerce."

146. Defendant's offer, provision, and/or sale of services at issue in this case are "consumer transaction[s]" within the scope of the FDUTPA. *See* Fla. Stat. §§ 501.201-501.213.

147. Plaintiff and the Nationwide Class, as "individual[s]," are "consumer[s]" as defined by the FDUTPA. *See* Fla. Stat. § 501.203(7).

148. Defendant provided services to Plaintiff and the Nationwide Class.

149. Defendant offered, provided, or sold services in Florida and engaged in trade or commerce directly or indirectly affecting the consuming public, within the meaning of the FDUTPA. *See* Fla. Stat. § 501.203.

150. Plaintiff and the Nationwide Class paid for or otherwise availed themselves and received services from Defendant, primarily for personal, family, or household purposes.

151. Defendant engaged in the conduct alleged in this Complaint, entering into transactions intended to result, and which did result, in the procurement or provision of employment or services to or from Plaintiff and the Nationwide Class.

152. Defendant's acts, practices, and omissions were done in the course of Defendant's businesses of offering, providing, and servicing customers throughout Florida and the United States.

153. The unfair, unconscionable, and unlawful acts and practices of Defendant alleged herein, and in particular the decisions regarding data security, emanated and arose within the State of Florida, within the scope of the FDUTPA.

154. Defendant, headquartered and operating in and out of Florida, engaged in unfair, unconscionable, and unlawful trade acts or practices in the conduct of trade or commerce, in violation of Fla. Stat. § 501.204(1), including but not limited to the following:

a. failure to implement and maintain reasonable and adequate computer systems and data security practices to safeguard PII;

b. omitting, suppressing, and concealing the material fact that their computer systems and data security practices were inadequate to safeguard PII from theft;

c. failure to protect the privacy and confidentiality of Plaintiff's and the Nationwide Class's PII;

d. continued acceptance and storage of PII after Defendant knew or should have known of the security vulnerabilities that were exploited in the Data Breach;

e. continued acceptance and storage of PII after Defendant knew or should have known of the Data Breach and before it allegedly remediated the Data Breach.

155. These unfair, unconscionable, and unlawful acts and practices violated duties imposed by laws, including by not limited to the FTC Act, 15 U.S.C. § 41, *et seq*., and the FDUTPA, Fla. Stat. § 501.171(2).

156. Defendant knew or should have known that its computer system and data security practices were inadequate to safeguard Plaintiff's and the Nationwide Class's PII and that the risk of a data breach or theft was high.

157. Plaintiff has standing to pursue this claim because as a direct and proximate result of Defendant's violations of the FDUTPA, Plaintiff and the Nationwide Class have been "aggrieved" by a violation of the FDUTPA and bring

this action to obtain a declaratory judgment that Defendant's acts or practices violate the FDUTPA. *See* Fla. Stat. § 501.211(a).

158. Plaintiff also has standing to pursue this claim because, as a direct result of Defendant's knowing violation of the FDUTPA, Plaintiff is at a substantial present and imminent risk of identity theft. Defendant still possesses Plaintiff's and the Nationwide Class's PII, and Plaintiff's PII was exfiltrated by unauthorized third parties, which is evidence of a substantial and imminent risk of future identity theft for all Plaintiff and the Nationwide Class.

159. Plaintiff and the Nationwide Class are entitled to injunctive relief to protect them from the substantial and imminent risk of future identity theft, including, but not limited to:

a. ordering that Defendant engage 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 prompt correction of any problems or issues detected by such third-party security auditors;

b. ordering that Defendant engage third-party security auditors and internal personnel to run automated security monitoring;

c. ordering that Defendant audit, test, and train security personnel regarding any new or modified procedures;

d. ordering that Defendant segment data by, among other things, creating firewalls and access controls so that if one area of a network system is compromised, hackers cannot gain access to other portions of the system;

e. ordering that Defendant purge, delete, and destroy PII not necessary for its provisions of services in a reasonably secure manner;

f. ordering that Defendant conduct regular database scans and security checks;

g. ordering that Defendant routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and

h. ordering Defendant to meaningfully educate individuals about the threats they face as a result of the loss of their financial and PII to third parties, as well as the steps victims should take to protect themselves.

160. Plaintiff brings this action on behalf of themselves and the Nationwide Class for the relief requested above and for the public benefit to promote the public

interests in the provision of truthful, fair information to allow employees and consumers to make informed purchasing decisions and to protect Plaintiff, the Nationwide Class, and the public from Defendant's unfair methods of competition and unfair, unconscionable, and unlawful practices. Defendant's wrongful conduct as alleged in this Complaint has had widespread impact on the public at large.

161. The above unfair, unconscionable, and unlawful practices and acts by Defendant were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to Plaintiff and the Nationwide Class that they could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

162. Defendant's actions and inactions in engaging in the unfair, unconscionable, and unlawful practices described herein were negligent, knowing and willful, and/or wanton and reckless.

163. Plaintiff and the Nationwide Class seek relief under the FDUTPA, Fla. Stat. §§ 501.201, *et seq*., including, but not limited to, a declaratory judgment that Defendant's actions and/or practices violate the FDUTPA.

164. Plaintiff and the Nationwide Class are also entitled to recover the costs of this action (including reasonable attorneys' fees) and such other relief as the Court deems just and proper.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of himself and Class Members, requests judgment against Defendant and that the Court grant the following:

A. For an Order certifying the Nationwide Class and appointing Plaintiff and his Counsel to represent each such Class;

B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of the PII of Plaintiff and Class Members, and from refusing to issue prompt, complete, any accurate disclosures to Plaintiff and Class Members;

C. For injunctive relief requested by Plaintiff, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and Class Members, including but not limited to an order:

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 personal identifying information of Plaintiff and 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 Plaintiff and Class Members;

iv. requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the PII of Plaintiff and Class Members;

v. prohibiting Defendant from maintaining the PII of Plaintiff and Class Members on a cloud-based database;

vi. 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;

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

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

ix. 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;

x. requiring Defendant to conduct regular database scanning and securing checks;

xi. 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 personal identifying information, as well as protecting the personal identifying information of Plaintiff and Class Members;

xii. requiring Defendant to routinely and continually conduct internal training and education, 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;

xiii. 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 personal identifying information;

xiv. 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;

xv. requiring Defendant to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves;

xvi. requiring Defendant to implement logging and monitoring programs sufficient to track traffic to and from Defendant's servers; and for a period of 10 years, appointing a qualified and independent third party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendant's compliance with the terms of the Court's final judgment, to provide such report to the Court and to

counsel for the class, and to report any deficiencies with compliance of the Court's final judgment;

D. For an award of damages, including actual, consequential, and nominal damages, as allowed by law in an amount to be determined;

E. For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;

F. For prejudgment interest on all amounts awarded; and

G. Such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiff hereby demands that this matter be tried before a jury.

Date: September 12, 2024

Respectfully Submitted,

/s/ Patrick A. Barthle, II
Patrick A. Barthle, II
MORGAN & MORGAN
COMPLEX LITIGATION GROUP
Florida Bar No. 99286
pbarthle@ForThePeople.com
201 N. Franklin Street, 7th Floor
Tampa, Florida 33602
Telephone: (813) 229-4023
Facsimile: (813) 222-4708

Ryan D. Maxey
MAXEY LAW FIRM, P.A.
107 N. 11th St. #402
Tampa, Florida 33602
Telephone: (813) 448-1125
Email: ryan@maxeyfirm.com

Attorney for Plaintiff and the Proposed Class

ClassAction.org
