UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF VIRGINIA
ROANOKE DIVISION

JANET HALL, on behalf of herself individually and on behalf of all others similarly situated, Plaintiff, v. PHYSICIANS TO WOMEN INC., Defendant.	**CASE NO.** 7:24cv00172 **CLASS ACTION COMPLAINT** **JURY DEMAND**

CLASS ACTION COMPLAINT

Plaintiff JANET HALL ("Plaintiff") brings this Class Action Complaint ("Complaint") against Defendant PHYSICIANS TO WOMEN INC., ("PTW" or "Defendant") as an individual and on behalf of all others similarly situated, and alleges, upon personal knowledge as to her own actions and her counsels' investigation, and upon information and belief as to all other matters, as follows:

NATURE OF THE ACTION

1. This Class Action arises from a recent cyberattack resulting in a data breach of sensitive information in the possession and custody and/or control of Defendant (the "Data Breach").

2. The Data Breach resulted in unauthorized disclosure, exfiltration, and theft of current and former patients' highly personal information, name, date of birth, telephone number, address, Social Security number, financial account information, ("personally identifying

information" or "PII"), and medical information, ("protected health information" or "PHI"). Plaintiff refers to both PII and PHI collectively as "Sensitive Information."

3. On information and belief, the Data Breach occurred on or about April 4, 2023. However, due to Defendant's inadequate cybersecurity, Defendant was unable to determine what types of patient information were accessed and acquired by the cybercriminal until July 5, 2023.

4. In or around January 26, 2024, PTW finally notified the state Attorneys General and many Class Members about the widespread Data Breach through a breach letter ("Notice Letter") as well as a website notice. However, notice is ongoing, with Plaintiff not receiving her Breach Notice until March 3, 2024. Plaintiff's breach notice is attached as Exhibit A.

5. PTW took an appalling nine months before informing Class Members even though Plaintiff and at least 147,000[1] of Class Members had their most sensitive personal information accessed, exfiltrated, and stolen, causing them to suffer ascertainable losses in the form of the loss of the benefit of their bargain and the value of their time reasonably incurred to remedy or mitigate the effects of the attack.

6. PTW's Breach Notice obfuscated the nature of the breach and the threat it posted—refusing to tell its patients how many people were impacted, how the breach happened, why it took Defendant over nine months to begin notifying victims that hackers had gained access to highly private Sensitive Information.

7. Defendant's failure to timely detect and report the Data Breach made its patients vulnerable to identity theft without any warnings to monitor their financial accounts or credit reports to prevent unauthorized use of their Sensitive Information.

[1]Roanoke Times, https://roanoke.com/news/local/crime-courts/lawsuit-roanoke-medical-office-could-have-prevented-data-breach/article_e2e024c4-d5ba-11ee-a3ed-57120be7bea5.html (last visited March 3, 2024).

8. Defendant knew or should have known that each victim of the Data Breach deserved prompt and efficient notice of the Data Breach and assistance in mitigating the effects of PII and PHI misuse.

9. In failing to adequately protect Plaintiff's and the Class's Sensitive Information, failing to adequately notify them about the breach, and by obfuscating the nature of the breach, Defendant violated state and federal law and harmed an unknown number of its current and former patients.

10. Plaintiff and members of the proposed Class are victims of Defendant's negligence and inadequate cyber security measures. Specifically, Plaintiff and members of the proposed Class trusted Defendant with their Sensitive Information. But Defendant betrayed that trust. Defendant failed to properly use up-to-date security practices to prevent the Data Breach.

11. Plaintiff a current PTW patient and Data Breach victim.

12. Accordingly, Plaintiff, on her own behalf and on behalf of a class of similarly situated individuals, brings this lawsuit seeking injunctive relief, damages, and restitution, together with costs and reasonable attorneys' fees, the calculation of which will be based on information in Defendant's possession.

PARTIES

13. Plaintiff, Janet Hall, is a natural person and citizen of Virginia, residing in Boones Mill, Virginia, where she intends to remain.

14. Defendant, PTW, is a Virginia corporation, with its principal place of business at 21 Highland Ave SE Ste 200, Roanoke, Virginia.

JURISDICTION AND VENUE

15. This Court has subject matter jurisdiction over this action under 28 U.S.C.§ 1332(d) because this is a class action wherein the amount in controversy exceeds the sum or value of $5,000,000, exclusive of interest and costs, there are more than 100 members in the proposed class. At least one member of the class is a citizen of a state different from Defendant.

16. This Court has personal jurisdiction over Defendant because Defendant maintains its principal place of business in this District and does substantial business in this District.

17. 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.

STATEMENT OF FACTS

PTW

18. PTW has specialized in obstetric and gynecological care since 1940[2] and currently boasts a total annual revenue of $13 million. [3]

19. As part of its business, PTW receives and maintains the Sensitive Information of thousands of current and former patients. In doing so, PTW implicitly promises to safeguard their Sensitive Information.

20. In collecting and maintaining its current and former patients' Sensitive Information, PTW agreed it would safeguard the data in accordance with state law, and federal law. After all, Plaintiff and Class Members themselves took reasonable steps to secure their Sensitive Information

[2] PTW, https://www.ptow.com/index.php (last visited March 3, 2024).
[3] PTW, Zoominfo, https://rocketreach.co/physicians-to-women-inc-profile_b5ce3d6af42e091f (last visited March 3, 2024).

21. Indeed, PTW acknowledges in its Privacy Policy that it is required to "maintain the privacy of your health information."[4]

22. Despite recognizing its duty to do so, on information and belief, PTW has not implemented reasonably cybersecurity safeguards or policies to protect its patients' Sensitive Information or supervised its IT or data security agents and employees to prevent, detect, and stop breaches of its systems. As a result, PTW leaves significant vulnerabilities in its systems for cybercriminals to exploit and gain access to patients' Sensitive Information.

The Data Breach

23. Plaintiff is a patient of PTW. As a condition of treatment with PTW, Plaintiff provided PTW with her Sensitive Information, including but not limited her name, Social Security Number, contact information, medical and health information, and date of birth. PTW used that Sensitive Information to facilitate its treatment of Plaintiff and required Plaintiff to provide that Sensitive Information to obtain treatment and care.

24. On information and belief, Defendant collects and maintains patients' Sensitive Information in its computer systems.

25. In collecting and maintaining Sensitive Information, Defendant implicitly agrees that it will safeguard the data using reasonable means according to state and federal law.

26. According to the Breach Notice, Defendant discovered "suspicious activity within [its] network" on April 4, 2023. Upon internal investigation, PTW discovered that "an unauthorized actor gained access to certain systems in [PTW's] network and acquired certain files from those systems[.]" Ex. A. In other words, Defendant's cyber and data security systems were

[4] Privacy Policy, PTW, https://www.ptow.com/ptow-formsandpolicies.php (last visited March 3, 2024).

so inadequate that it allowed cybercriminals to obtain and exfiltrate files containing a treasure trove of thousands of its patients' highly private Sensitive Information.

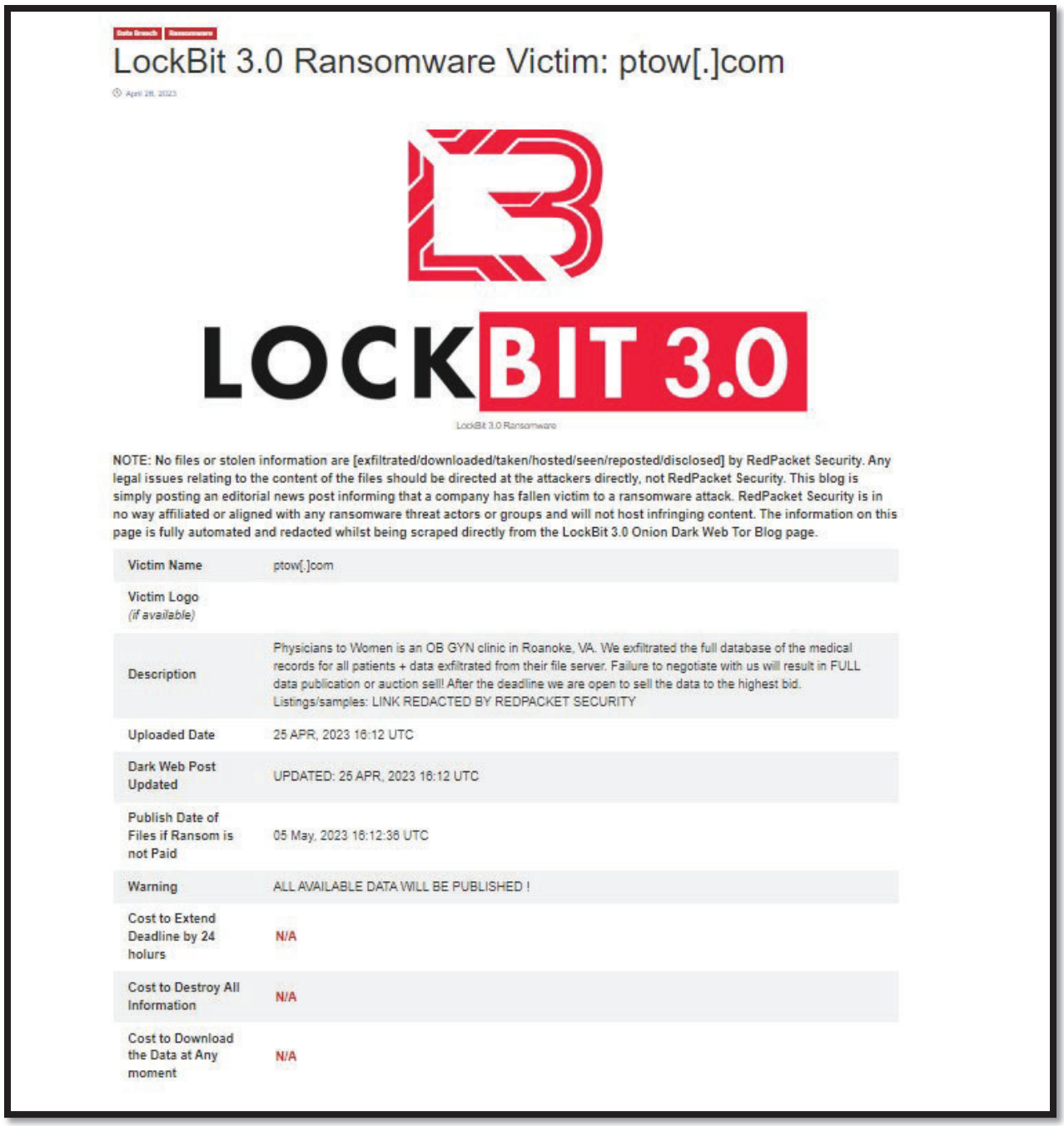
27. Through its inadequate security practices, Defendant exposed Plaintiff's and the Class's Sensitive Information for theft and sale on the dark web.

28. The notorious LockBit 3.0 ransomware gang claimed responsibility for the cyberattack on June 7, 2023. LockBit 3.0 is one of the most active ransomware actors, having breached over 1,000 companies worldwide[5] and PTW knew or should have known of the tactics that groups like LockBit 3.0 employ.

29. With the Sensitive Information secured and stolen by LockBit 3.0, the hackers then purportedly issued a ransom demand to PTW. However, PTW has provided no public information on the ransom demand or payment.

30. On information and belief, on May 5, 2023, the presumed deadline of LockBit 3.0's ransom demand, LockBit 3.0 released the "full database of medical records for all patients" on a data leak page.

[5] LockBit Hackers, BloomBerg, https://www.bloomberg.com/news/articles/2023-02-02/lockbit-hackers-behind-ion-breach-also-hit-royal-mail-hospital (last visited June 13, 2023).



Data Breach | Ransomware

LockBit 3.0 Ransomware Victim: ptow[.]com

April 28, 2023

LOCKBIT 3.0

LockBit 3.0 Ransomware

NOTE: No files or stolen information are [exfiltrated/downloaded/taken/hosted/seen/reposted/disclosed] by RedPacket Security. Any legal issues relating to the content of the files should be directed at the attackers directly, not RedPacket Security. This blog is simply posting an editorial news post informing that a company has fallen victim to a ransomware attack. RedPacket Security is in no way affiliated or aligned with any ransomware threat actors or groups and will not host infringing content. The information on this page is fully automated and redacted whilst being scraped directly from the LockBit 3.0 Onion Dark Web Tor Blog page.

Victim Name	ptow[.]com
Victim Logo *(if available)*	
Description	Physicians to Women is an OB GYN clinic in Roanoke, VA. We exfiltrated the full database of the medical records for all patients + data exfiltrated from their file server. Failure to negotiate with us will result in FULL data publication or auction sell! After the deadline we are open to sell the data to the highest bid. Listings/samples: LINK REDACTED BY REDPACKET SECURITY
Uploaded Date	25 APR, 2023 16:12 UTC
Dark Web Post Updated	UPDATED: 25 APR, 2023 16:12 UTC
Publish Date of Files if Ransom is not Paid	05 May, 2023 16:12:36 UTC
Warning	ALL AVAILABLE DATA WILL BE PUBLISHED !
Cost to Extend Deadline by 24 holurs	N/A
Cost to Destroy All Information	N/A
Cost to Download the Data at Any moment	N/A

31. On or around January 26, 2024–at least nine months after the Breach first occurred–PTW finally began notifying Class Members about the Data Breach.

32. Despite its duties and alleged commitments to safeguard Sensitive Information, Defendant did not in fact follow industry standard practices in securing patients' Sensitive Information, as evidenced by the Data Breach.

33. In response to the Data Breach, Defendant contends that it has "implemented additional security measures." Ex. A. Although Defendant fails to expand on what these alleged "measures" are, such measures should have been in place before the Data Breach.

34. Through its Breach Notice, Defendant also recognized the actual imminent harm and injury that flowed from the Data Breach, so it encouraged breach victims to "remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your free reports for suspicious activity[.]" Ex. A.

35. Defendant also recognized through its Breach Notice, its duty to implement safeguards in accordance with state law, and federal law, insisting that, despite the Breach showing otherwise, "the confidentiality, privacy, and security of personal information is among [its] highest priorities and [it has] strict security measures in place to protect information in [its] care." Defendant further pleads that it "sincerely regret[s] any inconvenience or concern this incident may cause you. Protecting your information is very important to [it], and [it] remain[s] committed to safeguarding the information in [its] care" Ex. A.

36. Cybercriminals need not harvest a person's Social Security number or financial account information in order to commit identity fraud or misuse Plaintiff's and the Class's Sensitive Information. Cybercriminals can cross-reference the data stolen from the Data Breach

and combine with other sources to create "Fullz" packages, which can then be used to commit fraudulent account activity on Plaintiff's and the Class's financial accounts.

37. On information and belief, PTW has offered several months of complimentary credit monitoring services to victims, which does not adequately address the lifelong harm that victims will face following the Data Breach. Indeed, the breach involves Sensitive Information that cannot be changed, such as Social Security numbers.

38. Even with several months' worth of credit monitoring services, the risk of identity theft and unauthorized use of Plaintiff's and Class Members' Sensitive Information is still substantially high. The fraudulent activity resulting from the Data Breach may not come to light for years.

39. On information and belief, Defendant failed to adequately train and supervise its IT and data security agents and employees on reasonable cybersecurity protocols or implement reasonable security measures, causing it to lose control over its patients' Sensitive Information. Defendant's negligence is evidenced by its failure to prevent the Data Breach and stop cybercriminals from accessing the Sensitive Information.

The Data Breach was a Foreseeable Risk of which Defendant was on Notice.

40. Defendant's data security obligations were particularly important given the substantial increase in cyberattacks and/or data breaches in the healthcare and healthcare adjacent industry preceding the date of the breach.

41. In light of recent high profile data breaches at other healthcare and healthcare adjacent companies, Defendant knew or should have known that its electronic records and patients' Sensitive Information would be targeted by cybercriminals.

42. In 2021, a record 1,862 data breaches occurred, resulting in approximately 293,927,708 sensitive records being exposed, a 68% increase from 2020.[6] The 330 reported breaches reported in 2021 exposed nearly 30 million sensitive records (28,045,658), compared to only 306 breaches that exposed nearly 10 million sensitive records (9,700,238) in 2020.[7]

43. Indeed, cyberattacks against the healthcare industry have become increasingly common for over ten years, with the FBI warning as early as 2011 that cybercriminals were "advancing their abilities to attack a system remotely" and "[o]nce a system is compromised, cyber criminals will use their accesses to obtain PII." The FBI further warned that that "the increasing sophistication of cyber criminals will no doubt lead to an escalation in cybercrime." [8]

44. Cyberattacks on medical systems and healthcare and healthcare adjacent companies like Defendant have become so notorious that the FBI and U.S. Secret Service have issued a warning to potential targets, so they are aware of, and prepared for, a potential attack. As one report explained, "[e]ntities like smaller municipalities and hospitals are attractive. . . because they often have lesser IT defenses and a high incentive to regain access to their data quickly."[9]

45. In fact, many high-profile ransomware attacks have occurred in healthcare and healthcare adjacent companies, with an estimated that nearly half of all ransomware attacks

[6] 2021 Data Breach Annual Report, ITRC, chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.wsav.com/wp-content/uploads/sites/75/2022/01/20220124_ITRC-2021-Data-Breach-Report.pdf (last visited January 10, 2024).
[7] *Id*.
[8] Gordon M. Snow Statement, FBI https://archives.fbi.gov/archives/news/testimony/cyber-security-threats-to-the-financial-sector (last visited January 10, 2024).
[9] Secret Service Warn of Targeted, Law360, https://www.law360.com/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware (last visited January 10, 2024).

being carried out are on healthcare companies, and with 85% of those attacks being ransomware similar to the one occurring here.[10]

46. Therefore, the increase in such attacks, and attendant risk of future attacks, was widely known to the public and to anyone in Defendant's industry, including PTW.

Plaintiff's Experience

47. Plaintiff is a PTW patient and a Data Breach victim, receiving the Data Breach notice on March 3, 2024.

48. As a condition of treatment with PTW, Plaintiff provided it with her Sensitive Information including her name, Social Security Number, contact information, medical and health information, and date of birth. PTW used that Sensitive Information to facilitate its treatment of Plaintiff and required Plaintiff to provide that Sensitive Information to obtain treatment and care.

49. Plaintiff provided her Sensitive Information to Defendant and trusted that it would use reasonable measures to protect it according to state and federal law.

50. Defendant deprived Plaintiff of the earliest opportunity to guard herself against the Data Breach's effects by failing to notify her about it for eleven months.

51. As a result of its inadequate cybersecurity, Defendant exposed Plaintiff's Sensitive Information for theft by cybercriminals and sale on the dark web.

52. 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

[10] Ransomware explained, CSO, https://www.csoonline.com/article/563507/what-is-ransomware-how-it-works-and-how-to-remove-it.html (last visited January 10, 2024);

Notice of Data Breach, self-monitoring her accounts and credit reports to ensure no fraudulent activity has occurred. This time has been lost forever and cannot be recaptured.

53. Plaintiff has and will spend considerable time and effort monitoring her accounts to protect herself from additional identity theft. Plaintiff fears for her personal financial security and uncertainty over what Sensitive Information was exposed in the Data Breach.

54. Plaintiff has and is experiencing feelings of anxiety, sleep disruption, stress, fear, and frustration because of the Data Breach. This goes far beyond allegations of mere worry or inconvenience; it is exactly the sort of injury and harm to a Data Breach victim that the law contemplates and addresses.

55. Plaintiff suffered actual injury in the form of damages to and diminution in the value of Plaintiff's Sensitive Information—a form of intangible property that Plaintiff entrusted to Defendant, which was compromised in and as a result of the Data Breach.

56. Plaintiff suffered actual injury from the exposure of her Sensitive Information —which violates her rights to privacy.

57. Plaintiff has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from her Sensitive Information being placed in the hands of unauthorized third parties and possibly criminals.

58. Indeed, following the Data Breach, between August and October 2023, Plaintiff suffered at least one fraudulent charge on her American Express card, ultimately forcing Plaintiff to replace her card.

59. Additionally, following the Data Breach Plaintiff has experienced an increase in spam calls, further suggesting that her Sensitive Information is now in the hands of cybercriminals.

60. Once an individual's PII is for sale and access on the dark web, as Plaintiff's PII is here as a result of the Breach, cybercriminals are able to use the stolen and compromised to gather and steal even more information.[11] On information and belief, Plaintiff's phone number and financial account were compromised as a result of the Data Breach.

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

Plaintiff and the Proposed Class Face Significant Risk of Continued Identity Theft

62. Plaintiff and members of the proposed Class have suffered injury from the misuse of their Sensitive Information that can be directly traced to Defendant.

63. As a result of Defendant's failure to prevent the Data Breach, Plaintiff and the proposed Class have suffered and will continue to suffer damages, including monetary losses, lost time, anxiety, and emotional distress. They have suffered or are at an increased risk of suffering:

a. The loss of the opportunity to control how their Sensitive Information is used;

b. The diminution in value of their Sensitive Information;

c. The compromise and continuing publication of their Sensitive Information;

[11] What do Hackers do with Stolen Information, Aura, https://www.aura.com/learn/what-do-hackers-do-with-stolen-information (last visited January 9, 2024).

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

e. Lost opportunity costs and lost wages associated with the time and effort expended 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;

f. Delay in receipt of tax refund monies;

g. Unauthorized use of stolen Sensitive Information; and

h. The continued risk to their Sensitive Information, which remains in Defendant's possession and is subject to further breaches so long as Defendant fails to undertake the appropriate measures to protect the Sensitive Information in its possession.

64. Stolen Sensitive Information is one of the most valuable commodities on the criminal information black market. According to Experian, a credit-monitoring service, stolen PII alone can be worth up to $1,000.00 depending on the type of information obtained.

65. The value of Plaintiff's and the Class's Sensitive Information on the black market is considerable. Stolen Sensitive Information trades on the black market for years, and criminals frequently post stolen Sensitive Information openly and directly on various "dark web" internet websites, making the information publicly available, for a substantial fee of course.

66. It can take victims years to spot identity theft, giving criminals plenty of time to use that information for cash.

67. One such example of criminals using Sensitive Information for profit is the development of "Fullz" packages.

68. Cyber-criminals can cross-reference two sources of Sensitive Information to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals. These dossiers are known as "Fullz" packages.

69. The development of "Fullz" packages means that stolen Sensitive Information from the Data Breach can easily be used to link and identify it to Plaintiff and the proposed Class' phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the Sensitive Information stolen by the cyber-criminals in the Data Breach, criminals can easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over. That is exactly what is happening to Plaintiff and members of the proposed Class, and it is reasonable for any trier of fact, including this Court or a jury, to find that Plaintiff's and the Class's stolen Sensitive Information is being misused, and that such misuse is fairly traceable to the Data Breach.

70. Defendant disclosed the Sensitive Information of Plaintiff and the Class for criminals to use in the conduct of criminal activity. Specifically, Defendant opened up, disclosed, and exposed the Sensitive Information of Plaintiff and the Class to people engaged in disruptive and unlawful business practices and tactics, including online account hacking, unauthorized use of financial accounts, and fraudulent attempts to open unauthorized financial accounts (i.e., identity fraud), all using the stolen Sensitive Information.

71. Defendant's failure to properly notify Plaintiff and members of the Class of the Data Breach exacerbated Plaintiff's and the Class's injury by depriving them of the earliest ability to take appropriate measures to protect their Sensitive Information and take other necessary steps to mitigate the harm caused by the Data Breach.

Defendant failed to adhere to FTC guidelines.

72. According to the Federal Trade Commission ("FTC"), the need for data security should be factored into all business decision-making. To that end, the FTC has issued numerous guidelines identifying best data security practices that businesses, such as Defendant, should employ to protect against the unlawful exposure of Sensitive Information.

73. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established guidelines for fundamental data security principles and practices for business. The guidelines explain that businesses should:

a. protect the sensitive consumer information that it keeps;

b. properly dispose of Sensitive Information that is no longer needed;

c. encrypt information stored on computer networks;

d. understand their network's vulnerabilities; and

e. implement policies to correct security problems.

74. The guidelines also recommend that businesses watch for large amounts of data being transmitted from the system and have a response plan ready in the event of a breach.

75. The FTC recommends that companies not maintain information 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.

76. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect consumer 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.

77. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to consumers' Sensitive Information constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

Defendant Violated HIPAA

78. HIPAA circumscribes security provisions and data privacy responsibilities designed to keep patients' medical information safe. HIPAA compliance provisions, commonly known as the Administrative Simplification Rules, establish national standards for electronic transactions and code sets to maintain the privacy and security of protected health information. [12]

79. HIPAA provides specific privacy rules that require comprehensive administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of PII and PHI is properly maintained.[13]

---

[12] HIPAA lists 18 types of information that qualify as PHI according to guidance from the Department of Health and Human Services Office for Civil Rights, and includes, inter alia: names, addresses, any dates including dates of birth, Social Security numbers, and medical record numbers.

[13] *See* 45 C.F.R. § 164.306 (security standards and general rules); 45 C.F.R. § 164.308 (administrative safeguards); 45 C.F.R. § 164.310 (physical safeguards); 45 C.F.R. § 164.312 (technical safeguards).

80. The Data Breach itself resulted from a combination of inadequacies showing Defendant's failure to comply with safeguards mandated by HIPAA. Defendant's security failures include, but are not limited to:

a. Failing to ensure the confidentiality and integrity of electronic PHI that it creates, receives, maintains and transmits in violation of 45 C.F.R. § 164.306(a)(1);

b. Failing to protect against any reasonably-anticipated threats or hazards to the security or integrity of electronic PHI in violation of 45 C.F.R. § 164.306(a)(2);

c. Failing to protect against any reasonably anticipated uses or disclosures of electronic PHI that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 C.F.R. § 164.306(a)(3);

d. Failing to ensure compliance with HIPAA security standards by Defendant in violation of 45 C.F.R. § 164.306(a)(4);

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

f. Failing to implement policies and procedures to prevent, detect, contain and correct security violations in violation of 45 C.F.R. § 164.308(a)(1);

g. Failing to identify and respond to suspected or known security incidents and failing to mitigate, to the extent practicable, harmful effects of security incidents

that are known to the covered entity in violation of 45 C.F.R. § 164.308(a)(6)(ii);

h. Failing to effectively train all staff members on the policies and procedures with respect to PHI as necessary and appropriate for staff members to carry out their functions and to maintain security of PHI in violation of 45 C.F.R. § 164.530(b) and 45 C.F.R. § 164.308(a)(5); and

i. Failing to design, implement, and enforce policies and procedures establishing physical and administrative safeguards to reasonably safeguard PHI, in compliance with 45 C.F.R. § 164.530(c).

81. Simply put, the Data Breach resulted from a combination of insufficiencies that demonstrate Defendant failed to comply with safeguards mandated by HIPAA regulations.

Defendant Fails to Comply with Industry Standards

82. As noted above, experts studying cyber security routinely identify entities in possession of PII and PHI as being particularly vulnerable to cyberattacks because of the value of the Sensitive Information which they collect and maintain.

83. Several best practices have been identified that a minimum should be implemented by employers in possession of PII and PHI, like Defendant, including but not limited to: educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data and limiting which employees can access sensitive data. Defendant failed to follow these industry best practices, including a failure to implement multi-factor authentication.

84. Other best cybersecurity practices that are standard for employers include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; training staff regarding critical points. Defendant failed to follow these cybersecurity best practices, including failure to train staff.

85. Defendant failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

86. Defendant also failed to meet the minimum standards of the Fair Information Practice Principles that Defendant cites to in its own Privacy Policy and refers to as the "backbone of privacy law in the United States" when establishing reasonable cybersecurity readiness. [14]

87. These foregoing frameworks are existing and applicable industry standards for an employer's obligations to provide adequate data security for its employees. Upon information and belief, Defendant failed to comply with at least one—or all—of these accepted standards, thereby opening the door to the threat actor and causing the Data Breach.

[14]FIPPs, FPC, https://www.fpc.gov/resources/fipps/#:~:text=Minimization.-,Agencies%20should%20only%20create%2C%20collect%2C%20use%2C%20process%2C%20store,Quality%20and%20Integrity (last visited June 5, 2023)

CLASS ACTION ALLEGATIONS

88. Plaintiff brings this class action under Fed. R. Civ. P. 23(a), 23(b)(2), and 23(b)(3), individually and on behalf of all members of the following class:

> All individuals residing whose Sensitive Information was compromised in the PTW Data Breach, including all those who received notice of the breach.

89. Excluded from the Class is Defendant, their agents, affiliates, parents, subsidiaries, any entity in which Defendant have a controlling interest, any of Defendant's officers or directors, any successors, and any Judge who adjudicates this case, including their staff and immediate family.

90. Plaintiff reserves the right to amend the class definition.

91. This action satisfies the numerosity, commonality, typicality, and adequacy requirements under Fed. R. Civ. P. 23.

a. **Numerosity**. Plaintiff is representative of the Class, consisting of at least 147,000 members, far too many to join in a single action;

b. **Ascertainability**. Members of the Class are readily identifiable from information in Defendant's possession, custody, and control;

c. **Typicality**. Plaintiff's claims are typical of class claims as each arises from the same Data Breach, the same alleged violations by Defendant, and the same unreasonable manner of notifying individuals about the Data Breach.

d. **Adequacy**. Plaintiff will fairly and adequately protect the proposed Class's interests. Her interests do not conflict with the Class's interests, and she has retained counsel experienced in complex class action litigation and data privacy to prosecute this action on the Class's behalf, including as lead counsel.

e. **Commonality**. Plaintiff's and the Class's claims raise predominantly common fact and legal questions that a class wide proceeding can answer for the Class. Indeed, it will be necessary to answer the following questions:

i. Whether Defendant had a duty to use reasonable care in safeguarding Plaintiff's and the Class's Sensitive Information;

ii. 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;

iii. Whether Defendant were negligent in maintaining, protecting, and securing Sensitive Information;

iv. Whether Defendant breached contract promises to safeguard Plaintiff's and the Class's Sensitive Information;

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

vi. Whether Defendant's Breach Notice was reasonable;

vii. Whether the Data Breach caused Plaintiff's and the Class's injuries;

viii. What the proper damages measure is; and

ix. Whether Plaintiff and the Class are entitled to damages, treble damages, or injunctive relief.

92. Further, common questions of law and fact predominate over any individualized questions, and a class action is superior to individual litigation or any other available method to fairly and efficiently adjudicate the controversy. The damages available to individual plaintiffs are insufficient to make individual lawsuits economically feasible.

COUNT I
Negligence
(On Behalf of Plaintiff and the Class)

93. Plaintiff realleges all previous paragraphs as if fully set forth below.

94. Plaintiff and members of the Class entrusted their Sensitive Information to Defendant. Defendant owed to Plaintiff and the Class a duty to exercise reasonable care in handling and using the Sensitive Information in its care and custody, including implementing industry-standard security procedures sufficient to reasonably protect the information from the Data Breach, theft, and unauthorized use that came to pass, and to promptly detect attempts at unauthorized access.

95. Defendant owed a duty of care to Plaintiff and members of the Class because it was foreseeable that Defendant's failure to adequately safeguard their Sensitive Information in accordance with state-of-the-art industry standards concerning data security would result in the compromise of that Sensitive Information —just like the Data Breach that ultimately came to pass. Defendant acted with wanton and reckless disregard for the security and confidentiality of Plaintiff's and the Class's Sensitive Information by disclosing and providing access to this information to unauthorized third parties and by failing to properly supervise both the way the Sensitive Information was stored, used, and exchanged, and those in its employ who were responsible for making that happen.

96. Defendant owed to Plaintiff and members of the Class a duty to notify them within a reasonable timeframe of any breach to the security of their Sensitive Information. Defendant also owed a duty to timely and accurately disclose to Plaintiff and members of the Class the scope, nature, and occurrence of the Data Breach. This duty is required and necessary for Plaintiff and the Class to take appropriate measures to protect their Sensitive Information,

to be vigilant in the face of an increased risk of harm, and to take other necessary steps to mitigate the harm caused by the Data Breach.

97. Defendant owed these duties to Plaintiff and members of the Class because they are members of a well-defined, foreseeable, and probable class of individuals whom Defendant knew or should have known would suffer injury-in-fact from Defendant's inadequate security protocols. Defendant actively sought and obtained Plaintiff's and the Class's Sensitive Information.

98. The risk that unauthorized persons would attempt to gain access to the Sensitive Information and misuse it was foreseeable. Given that Defendant holds vast amounts of Sensitive Information, it was inevitable that unauthorized individuals would attempt to access Defendant's databases containing the Sensitive Information —whether by malware or otherwise.

99. Sensitive Information is highly valuable, and Defendant knew, or should have known, the risk in obtaining, using, handling, emailing, and storing the Sensitive Information of Plaintiff and the Class and the importance of exercising reasonable care in handling it.

100. Defendant breached its duties by failing to exercise reasonable care in supervising its employees, agents, contractors, vendors, and suppliers, and in handling and securing the Sensitive Information of Plaintiff and the Class which actually and proximately caused the Data Breach and Plaintiff's and the Class's injury. Defendant further breached its duties by failing to provide reasonably timely notice of the Data Breach to Plaintiff and members of the Class, which actually and proximately caused and exacerbated the harm from the Data Breach and Plaintiff's and members of the Class's injuries-in-fact. As a direct and traceable result of Defendant's negligence and/or negligent supervision, Plaintiff and the Class

have suffered or will suffer damages, including monetary damages, increased risk of future harm, embarrassment, humiliation, frustration, and emotional distress.

101. Defendant's breach of its common-law duties to exercise reasonable care and its failures and negligence actually and proximately caused Plaintiff and members of the Class actual, tangible, injury-in-fact and damages, including, without limitation, the theft of their Sensitive Information by criminals, improper disclosure of their Sensitive Information, lost benefit of their bargain, lost value of their Sensitive Information, and lost time and money incurred to mitigate and remediate the effects of the Data Breach that resulted from and were caused by Defendant's negligence, which injury-in-fact and damages are ongoing, imminent, immediate, and which they continue to face.

COUNT II
Negligence *Per Se*
(On Behalf of Plaintiff and the Class)

102. Plaintiff realleges all previous paragraphs as if fully set forth below.

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

104. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect customers or, in this case, patients' Sensitive Information. The FTC publications and orders promulgated pursuant to the FTC Act also form part of the basis of Defendant's duty to protect Plaintiff's and the members of the Class's Sensitive Information.

105. Defendant breached its duties to Plaintiff and Class Members under the FTC Act by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Sensitive Information.

106. Defendant's duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendant and its patients, which is recognized by laws and regulations including but not limited to HIPAA, as well as common law. Defendant was in a position to ensure that its systems were sufficient to protect against the foreseeable risk of harm to Class Members from a Data Breach.

107. Defendant's duty to use reasonable security measures under HIPAA required Defendant to "reasonably protect" confidential data from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 45 C.F.R. § 164.530(c)(l). Some or all of the healthcare and/or medical information at issue in this case constitutes "protected health information" within the meaning of HIPAA.

108. Defendant's duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendant is bound by industry standards to protect confidential Sensitive Information.

109. Defendant violated its duty under Section 5 of the FTC Act by failing to use reasonable measures to protect Plaintiff's and the Class's Sensitive Information and not complying with applicable industry standards as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of Sensitive Information Defendant collected and stored and the foreseeable consequences of a data breach, including,

specifically, the immense damages that would result to individuals in the event of a breach, which ultimately came to pass.

110. The harm that has occurred is the type of harm the FTC Act is intended to guard against. Indeed, the FTC has pursued numerous enforcement actions against businesses that, because of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and the Class.

111. Defendant violated its duty under HIPAA by failing to use reasonable measures to protect their PHI and by not complying with applicable regulations detailed supra. Here too, Defendant's conduct was particularly unreasonable given the nature and amount of Sensitive Information Defendant collected and stored and the foreseeable consequences of a data breach, including, specifically, the immense damages that would result to individuals in the event of a breach, which ultimately came to pass.

112. But for Defendant's wrongful and negligent breach of the duties owed to Plaintiff and members of the Class, Plaintiff and members of the Class would not have been injured.

113. The injury and harm suffered by Plaintiff and members of the Class were the reasonably foreseeable result of Defendant's breach of its duties. Defendant knew or should have known that it was failing to meet its duties and that its breach would cause Plaintiff and members of the Class to suffer the foreseeable harms associated with the exposure of their Sensitive Information.

114. Had Plaintiff and the Class known that Defendant did not adequately protect their Sensitive Information, Plaintiff and members of the Class would not have entrusted Defendant with their Sensitive Information.

115. Defendant's various violations and its failure to comply with applicable laws and regulations constitutes negligence *per se*.

116. As a direct and proximate result of Defendant's negligence *per se*, Plaintiff and the Class have suffered harm, including loss of time and money resolving fraudulent charges; loss of time and money obtaining protections against future identity theft; lost control over the value of Sensitive Information; harm resulting from damaged credit scores and information; and other harm resulting from the unauthorized use or threat of unauthorized use of stolen Sensitive Information, entitling them to damages in an amount to be proven at trial.

117. Additionally, as a direct and proximate result of Defendant's negligence *per se*, Plaintiff and Class members have suffered and will suffer the continued risks of exposure of their Sensitive Information, 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 their Sensitive Information in its continued possession.

COUNT III
Breach of an Implied Contract
(On Behalf of Plaintiff and the Class)

118. Plaintiff realleges all previous paragraphs as if fully set forth below.

119. Plaintiff and the Class delivered their Sensitive Information to Defendant as part of the process of obtaining treatment and services provided by Defendant.

120. Plaintiff and Class Members entered into implied contracts with Defendant under which Defendant agreed to safeguard and protect such information and to timely and accurately notify Plaintiff and Class Members if and when their data had been breached and compromised. Each such contractual relationship imposed on Defendant an implied covenant of good faith and fair dealing by which Defendant was required to perform its obligations and

manage Plaintiff's and Class Members' data in a manner which comported with the reasonable expectations of privacy and protection attendant to entrusting such data to Defendant.

121. In providing their Sensitive Information, Plaintiff and Class Members entered into an implied contract with Defendant whereby Defendant, in receiving such data, became obligated to reasonably safeguard Plaintiff's and the other Class Members' Sensitive Information.

122. In delivering their Sensitive Information to Defendant, Plaintiff and Class Members intended and understood that Defendant would adequately safeguard that data.

123. Plaintiff and the Class Members would not have entrusted their Sensitive Information to Defendant in the absence of such an implied contract.

124. Defendant accepted possession of Plaintiff's and Class Members' Sensitive Information.

125. Had Defendant disclosed to Plaintiff and Class Members that Defendant did not have adequate computer systems and security practices to secure patients' Sensitive Information, Plaintiff and members of the Class would not have provided their Sensitive Information to Defendant.

126. Defendant recognized that patients' Sensitive Information is highly sensitive and must be protected, and that this protection was of material importance as part of the bargain to Plaintiff and Class Members.

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

128. Defendant breached the implied contract with Plaintiff and Class Members by failing to take reasonable measures to safeguard its data.

129. Defendant breached the implied contract with Plaintiff and Class Members by failing to promptly notify them of the access to and exfiltration of their Sensitive Information.

130. As a direct and proximate result of the breach of the contractual duties, Plaintiff and Class Members have suffered actual, concrete, and imminent injuries. The injuries suffered by Plaintiff and the Class Members include: (a) the invasion of privacy; (b) the compromise, disclosure, theft, and unauthorized use of Plaintiff's and Class Members' Sensitive Information; (c) economic costs associated with the time spent to detect and prevent identity theft, including loss of productivity; (d) monetary costs associated with the detection and prevention of identity theft; (e) economic costs, including time and money, related to incidents of actual identity theft; (f) the emotional distress, fear, anxiety, nuisance and annoyance of dealing related to the theft and compromise of their Sensitive Information; (g) the diminution in the value of the services bargained for as Plaintiff and Class Members were deprived of the data protection and security that Defendant promised when Plaintiff and the proposed class entrusted Defendant with their Sensitive Information; and (h) the continued and substantial risk to Plaintiff's and Class Members' Sensitive Information, which remains in the Defendant's possession with inadequate measures to protect Plaintiff's and Class Members' Sensitive Information.

COUNT IV
Unjust Enrichment
(On Behalf of Plaintiff and the Class)

131. Plaintiff realleges all previous paragraphs as if fully set forth below.

132. This claim is pleaded in the alternative to the breach of implied contractual duty claim.

133. Plaintiff and members of the Class conferred a benefit upon Defendant in providing Sensitive Information to Defendant.

134. Defendant appreciated or had knowledge of the benefits conferred upon it by Plaintiff and the Class. Defendant also benefited from the receipt of Plaintiff's and the Class's Sensitive Information, as this was used to facilitate the treatment, services, and goods it sold to Plaintiff and the Class.

135. Under principles of equity and good conscience, Defendant should not be permitted to retain the full value of Plaintiff and the Class's Sensitive Information because Defendant failed to adequately protect their Sensitive Information. Plaintiff and the proposed Class would not have provided their Sensitive Information to Defendant had they known Defendant would not adequately protect their Sensitive Information.

136. Defendant should be compelled to disgorge into a common fund for the benefit of Plaintiff and members of the Class all unlawful or inequitable proceeds received by them because of their misconduct and Data Breach.

COUNT V
Breach of Fiduciary Duty
(On Behalf of Plaintiff and the Class)

137. Plaintiff realleges all previous paragraphs as if fully set forth below.

138. Given the relationship between Defendant and Plaintiff and Class Members, where Defendant became guardian of Plaintiff's and Class Members' Sensitive Information, Defendant became a fiduciary by its undertaking and guardianship of the Sensitive Information, to act primarily for Plaintiff and Class Members, (1) for the safeguarding of Plaintiff's and Class Members' Sensitive Information; (2) to timely notify Plaintiff and Class

Members of a Data Breach and disclosure; and (3) to maintain complete and accurate records of what information (and where) Defendant did and does store.

139. Defendant has a fiduciary duty to act for the benefit of Plaintiff and Class Members upon matters within the scope of Defendant's relationship with them—especially to secure their Sensitive Information.

140. Because of the highly sensitive nature of the Sensitive Information, Plaintiff and Class Members would not have entrusted Defendant, or anyone in Defendant's position, to retain their Sensitive Information had they known the reality of Defendant's inadequate data security practices.

141. Defendant breached its fiduciary duties to Plaintiff and Class Members by failing to sufficiently encrypt or otherwise protect Plaintiff's and Class Members' Sensitive Information.

142. Defendant also breached its fiduciary duties to Plaintiff and Class Members by failing to diligently discover, investigate, and give notice of the Data Breach in a reasonable and practicable period.

143. As a direct and proximate result of Defendant's breach of its fiduciary duties, Plaintiff and Class Members have suffered and will continue to suffer numerous injuries (as detailed *supra*).

PRAYER FOR RELIEF

Plaintiff and the Class demand a jury trial on all claims so triable and request that the Court enter an order:

A. Certifying this case as a class action on behalf of Plaintiff and the proposed Class, appointing Plaintiff as class representatives, and appointing their counsel to represent the Class;

B. Awarding declaratory and other equitable relief as is necessary to protect the interests of Plaintiff and the Class;

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

D. Enjoining Defendant from further deceptive practices and making untrue statements about the Data Breach and the stolen Sensitive Information;

E. Awarding Plaintiff and the Class damages that include applicable compensatory, exemplary, punitive damages, and statutory damages, as allowed by law;

F. Awarding restitution and damages to Plaintiff and the Class in an amount to be determined at trial;

G. Awarding attorneys' fees and costs, as allowed by law;

H. Awarding prejudgment and post-judgment interest, as provided by law;

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

J. Granting such other or further relief as may be appropriate under the circumstances.

Dated: March 7, 2024

Respectfully submitted,

By: /s/ *Lee A. Floyd*
Lee A. Floyd (VSB #88459)
Sarah G. Sauble (VSB #94757)
BREIT BINIAZAN, PC

2100 E. Cary Street, Suite 310
Richmond, Virginia 23223
(804) 351-9040
(757) 670-3939
Lee@bbtrial.com
Sarah@bbtrial.com

Samuel J. Strauss (*pro hac vice* pending)
Raina Borrelli (*pro hac vice* pending)
TURKE & STRAUSS LLP
613 Williamson Street, Suite 201
Madison, Wisconsin 53703
Telephone: (608) 237-1775
Facsimile: (608) 509-4423
sam@turkestrauss.com
raina@turkestrauss.com

Attorneys for Plaintiff and Proposed Class