STATE OF RHODE ISLAND JUDICIARY

SUPERIOR COURT

SUMMONS

	Civil Action File Number KC-2025-0098
Plaintiff Bonnie Felingiere v. Orthopedics Rhode Island, Inc. **Defendant**	**Attorney for the Plaintiff or the Plaintiff** Christopher E Hultquist **Address of the Plaintiff's Attorney or the Plaintiff** 56 PINE STREET SUITE 200 PROVIDENCE RI 02903
Noel Judicial Complex Kent County 222 Quaker Lane Warwick RI 02886 (401) 822-6900	**Address of the Defendant** 200 Crossings Boulevard Suite 500 Warwick RI 02886

TO THE DEFENDANT, Orthopedics Rhode Island, Inc.:

The above-named Plaintiff has brought an action against you in said Superior Court in the county indicated above. You are hereby summoned and required to serve upon the Plaintiff's attorney, whose address is listed above, an answer to the complaint which is herewith served upon you within twenty (20) days after service of this Summons upon you, exclusive of the day of service.

If you fail to do so, judgment by default will be taken against you for the relief demanded in the complaint. Your answer must also be filed with the court.

As provided in Rule 13(a) of the Superior Court Rules of Civil Procedure, unless the relief demanded in the complaint is for damage arising out of your ownership, maintenance, operation, or control of a motor vehicle, or unless otherwise provided in Rule 13(a), your answer must state as a counterclaim any related claim which you may have against the Plaintiff, or you will thereafter be barred from making such claim in any other action.

This Summons was generated on 1/24/2025.	/s/ Danielle Keegan Clerk

Witness the seal/watermark of the Superior Court

A true copy attest
Robert J. Kilduff #6070
Date 1/28/25

STATE OF RHODE ISLAND JUDICIARY

SUPERIOR COURT

Plaintiff	**Civil Action File Number**
Bonnie Felingiere v. Orthopedics Rhode Island, Inc. **Defendant**	KC-2025-0098

PROOF OF SERVICE

I hereby certify that on the date below I served a copy of this Summons, complaint, Language Assistance Notice, and all other required documents received herewith upon the Defendant, Orthopedics Rhode Island, Inc., by delivering or leaving said papers in the following manner:

☐ With the Defendant personally.

☐ At the Defendant's dwelling house or usual place of abode with a person of suitable age and discretion then residing therein.
Name of person of suitable age and discretion _____
Address of dwelling house or usual place of abode _____
_____
Age _____
Relationship to the Defendant _____

☐ With an agent authorized by appointment or by law to receive service of process.
Name of authorized agent _____
If the agent is one designated by statute to receive service, further notice as required by statute was given as noted below.
_____

☐ With a guardian or conservator of the Defendant.
Name of person and designation _____

☐ By delivering said papers to the attorney general or an assistant attorney general if serving the state.

☐ Upon a public corporation, body, or authority by delivering said papers to any officer, director, or manager.
Name of person and designation _____

STATE OF RHODE ISLAND JUDICIARY

SUPERIOR COURT

Upon a private corporation, domestic or foreign:

☐ By delivering said papers to an officer or a managing or general agent.
Name of person and designation _____

☐ By leaving said papers at the office of the corporation with a person employed therein.
Name of person and designation _____

☐ By delivering said papers to an agent authorized by appointment or by law to receive service of process.
Name of authorized agent _____
If the agent is one designated by statute to receive service, further notice as required by statute was given as noted below.

_____

☐ I was unable to make service after the following reasonable attempts: _____

_____

SERVICE DATE: ____/____/____ (Month Day Year) | SERVICE FEE $_____

Signature of SHERIFF or DEPUTY SHERIFF or CONSTABLE

SIGNATURE OF PERSON OTHER THAN A SHERIFF or DEPUTY SHERIFF or CONSTABLE MUST BE NOTARIZED.

_____
Signature

State of _____
County of _____

On this _____ day of _____, 20____, before me, the undersigned notary public, personally appeared _____ ☐ personally known to the notary or ☐ proved to the notary through satisfactory evidence of identification, which was _____, to be the person who signed above in my presence, and who swore or affirmed to the notary that the contents of the document are truthful to the best of his or her knowledge.

Notary Public: _____
My commission expires: _____
Notary identification number: _____

STATE OF RHODE ISLAND **SUPERIOR COURT**
KENT, SC.

Bonnie Felingiere,	)	
	)	
Plaintiff,	)	Case No.
	)	
v.	)	
	)	
Orthopedics Rhode Island, Inc.	)	
	)	
Defendant	)	
	)	

CLASS ACTION COMPLAINT

Plaintiff Bonnie Felingiere, individually and on behalf of all others similarly situated, for her Class Action Complaint, brings this action against Defendant Orthopedics Rhode Island ("Ortho RI") based on personal knowledge and the investigation of counsel and alleges as follows:

I. INTRODUCTION

1. Between September 4, 2024 and September 7, 2024, an unknown actor gained access to Defendant's inadequately protected computer systems. As a result, Plaintiff and the Class Members (as further defined below) have had their personal identifiable information ("PII")[1] and private health information ("PHI") including their names, addresses, dates of birth, billing and claims information, health insurance information, and medical information including diagnoses, medications, test results, x-ray images and other treatment information (collectively, "Private Information"), exposed (the "Data Breach").

2. Ortho RI provides medical services across the state of Rhode Island.

[1] Personal 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.

3. Plaintiff and members of the class are or were patients at Ortho RI.

4. In carrying out its business, Defendant obtains, collects, uses, and derives a benefit from the PII/PHI of Plaintiff and the Class. As such, Defendant assumed the legal and equitable duties to those individuals to protect and safeguard that information from unauthorized access and intrusion.

5. Due to Defendant's negligence, cybercriminals obtained everything they need to commit identity theft and wreak havoc on the financial and personal lives of thousands of individuals.

6. This class action seeks to redress Defendant's unlawful, willful and wanton failure to protect the Private Information of hundreds of individuals that was exposed in a major data breach of Defendant's network in violation of its legal obligations.

7. For the rest of their lives, Plaintiff and the Class Members will have to deal with the danger of identity thieves possessing and misusing their PII/PHI. Plaintiff and Class Members will have to spend time responding to the Breach and are at an immediate, imminent, and heightened risk of all manners of identity theft as a direct and proximate result of the Data Breach. Plaintiff and Class Members have incurred and/or will continue to incur damages in the form of, among other things, identity theft, attempted identity theft, lost time and expenses mitigating harms, increased risk of harm, damaged credit, deprivation of the value of their PII/PHI, loss of privacy, and/or additional damages as described below.

8. Defendant betrayed the trust of Plaintiff and the other Class Members by failing to properly safeguard and protect their personal identifiable information and thereby enabling cybercriminals to steal such valuable and sensitive information.

9. Plaintiff brings this action individually and on behalf of the Class, seeking remedies including, but not limited to, compensatory damages, reimbursement of out-of-pocket costs, injunctive relief, reasonable attorney fees and costs, and all other remedies this Court deems proper.

II. THE PARTIES

10. Plaintiff Felingiere is a resident of West Warwick, Rhode Island.

11. Ortho RI is incorporated in Rhode Island and headquartered in Warwick, RI.

12. 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.

13. 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

14. This Court has subject matter jurisdiction over this case.

15. Defendant is a citizen of Rhode Island because it is incorporated in Rhode Island with its principal place of business in Rhode Island.

16. This Court has personal jurisdiction over Defendant because it conducts substantial business in Rhode Island and this District and collected and/or stored the PII/PHI of Plaintiff and Class Members in this District.

17. Venue is proper in this District because Defendant operates in this District and a substantial part of the events or omissions giving rise to Plaintiff and the Class Members' claims

occurred in this District, including Defendant collecting and/or storing the PII/PHI of Plaintiff and Class Members.

IV. FACTUAL ALLEGATIONS

Background

18. Ortho RI has eight offices across Rhode Island.

19. In order to provide medical services, Defendant requires Plaintiff's and Class Members' PII/PHI, including their names, dates of birth, email addresses, physical addresses, Social Security numbers, financial account information, health insurance information, and medical history.

20. Defendant collected, stored, and maintained the PII/PHI of Plaintiff and the Class Members on its network. Defendant, however, failed to take reasonable and necessary steps to ensure that its network was secure.

21. By obtaining, collecting, and storing the PII/PHI 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/PHI from disclosure.

22. Plaintiff and the Class Members did not have control over how Defendant stored and maintained their PII/PHI. Rather, Plaintiff was at Defendant's mercy, as Defendant had sole control and authority over its protection of Plaintiff's and the Class Members' PII/PHI.

23. Plaintiff and Class Members have taken reasonable steps to maintain the confidentiality of their PII/PHI and relied on Defendant to keep their PII/PHI confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

24. Plaintiff and other Members of the Class entrusted their PII/PHI to Defendant.

25. Plaintiff and Class Members relied on this sophisticated Defendant to keep their PII/PHI confidential and securely maintained, to use for information for business purposes only, and to only make authorized disclosures of this information. Plaintiff and Class Members demanded security to safeguard their PII/PHI.

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

27. Despite recognizing its duty to do so, on information and belief, Defendant has not implemented reasonable cybersecurity safeguards or policies to protect its consumers' PII/PHI or trained its IT or data security employees to prevent, detect, and stop breaches of its systems. Rather, Defendant chose to store Plaintiff's and the Class Members' PII/PHI on an unsecure network, leaving their PII/PHI vulnerable for cybercriminals to take. As a result, Defendant leaves significant vulnerabilities in its systems for cybercriminals to exploit and gain access to patients' PII/PHI.

The Data Breach

28. Between September 4, 2024 and September 7, 2024, due to Defendant's failure to maintain an adequate security system, an unknown hacker gained access to Defendant's systems and acquired certain files and information including Plaintiff and Class Members' PII.

29. Defendant failed to timely detect the Data Breach until September 6, 2024. Even then, Defendant filed to stop the spread of the Data Breach until the next day. During that time, an unknown cybercriminal was able to access files and folders containing Plaintiff's and the Class Members' PII/PHI.

30. The targeted cyberattack was expressly designed to gain access to and exfiltrate private and confidential data, including (among other things) the PII/PHI of patients like Plaintiff and Class Members.

31. Defendant negligently delayed in responding to the notice and did not conclude its review of the attack until November 6, 2024. Upon information and belief, Defendant is still investigating the Data Breach.

32. Defendant filed a notice of the Data Breach with the U.S. Department of Health and Human Services Office for Civil Rights. In that notice, Defendant admitted that an unauthorized actor accessed sensitive information about Plaintiff and the Class Members.

33. 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 have not been shared with regulators or Plaintiff and Class Members, who retain a vested interest in ensuring that their information remains protected.

34. The unencrypted PII/PHI 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/PHI for targeted marketing without the approval of Plaintiff and Class Members. Unauthorized individuals can easily access the PII/PHI of Plaintiff and Class Members.

35. Defendant was negligent and 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/PHI for Plaintiff and Class Members.

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

37. Defendant breached its obligations to Plaintiff and Class Members and/or was otherwise negligent and reckless because it failed to properly maintain and safeguard its computer systems and data. Defendant's unlawful conduct includes, but is not limited to, the following acts and/or omissions:

a. Failing to maintain an adequate data security system to reduce the risk of data breaches and cyber-attacks;

b. Failing to adequately protect patients' and customers' PII/PHI;

c. Failing to properly monitor its own data security systems for existing intrusions;

d. Failing to ensure that its vendors with access to its computer systems and data employed reasonable security procedures;

e. Failing to train its employees in the proper handling of emails containing Private Information and maintain adequate email security practices;

f. Failing to ensure the confidentiality and integrity of electronic PII/PHI it created, received, maintained, and/or transmitted, in violation of 45 C.F.R. § 164.306(a)(1);

g. Failing to implement technical policies and procedures for electronic information systems that maintain electronic PII/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);

h. 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)(i);

i. Failing to implement procedures to review records of information system

activity regularly, such as audit logs, access reports, and security incident tracking reports in violation of 45 C.F.R. § 164.308(a)(1)(ii)(D);

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

k. Failing to protect against reasonably anticipated uses or disclosures of electronic PII/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);

l. Failing to ensure compliance with HIPAA security standard rules by its workforces in violation of 45 C.F.R. § 164.306(a)(4);

m. Failing to train all members of its workforces effectively on the policies and procedures regarding PII/PHI as necessary and appropriate for the members of its workforces to carry out their functions and to maintain security of PHI, in violation of 45 C.F.R. § 164.530(b);

n. Failing to render the electronic PII/PHI it maintained unusable, unreadable, or indecipherable to unauthorized individuals, as it had not encrypted the electronic PII/PHI as specified in the HIPAA Security Rule by "the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key" (45 CFR § 164.304's definition of "encryption");

o. Failing to comply with FTC guidelines for cybersecurity, in violation of Section 5 of the FTC Act;

p. Failing to adhere to industry standards for cybersecurity as discussed above; and

q. Otherwise breaching its duties and obligations to protect Plaintiff's and Class Members' Private Information.

38. Defendant negligently and unlawfully failed to safeguard Plaintiff's and Class Members' PII/PHI by allowing cyberthieves to access Defendant's computer network and systems which contained unsecured and unencrypted PII/PHI.

39. Accordingly, Plaintiff and Class Members now face an increased risk of fraud and identity theft. In addition, Plaintiff and the Class Members also lost the benefit of the bargain they made with Defendant.

The Data Breach was Foreseeable

40. In the years and months immediately preceding the Data Breach, Defendant knew or should have known that Defendant's computer systems were a target for cybersecurity attacks 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

[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).

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

44. Medical facilities, such as Defendant, collect and store large amounts of critical, highly valuable corporate records.

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

46. Considering the information readily available and accessible on the internet before the Data Breach, Defendant, having elected to store the unencrypted PII/PHI of Plaintiff and Class Members in an Internet-accessible environment, had reason to be on guard for the exfiltration of

---

[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).

[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).

the PII, and Defendant's type of business had cause to be particularly on guard against such an attack.

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

48. 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/PHI to protect against their publication and misuse in the event of a cyberattack.

The Data Breach was Preventable

49. By obtaining, collecting, and storing the PII/PHI 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/PHI from disclosure.

50. Plaintiff and Class Members have taken reasonable steps to maintain the confidentiality of their PII/PHI and relied on Defendant to keep their PII/PHI confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

51. As explained by the Federal Bureau of Investigation, "[p]revention is the most effective defense against ransomware and it is critical to take precautions for protection."[5]

52. To prevent and detect ransomware attacks, including the ransomware attack that resulted in the Data Breach, Defendant could and should have implemented, as recommended by the United States Government, the following measures:

---

[5] See How to Protect Your Networks from RANSOMWARE, at 3, available at https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view (last visited July 17, 2023).

- Implement an awareness and training program. Because end users are targets, employees and individuals should be aware of the threat of ransomware and how it is delivered.

- Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.

- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.

- Configure firewalls to block access to known malicious IP addresses.

- Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system.

- Set anti-virus and anti-malware programs to conduct regular scans automatically.

- Manage the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.

- Configure access controls—including file, directory, and network share permissions—with least privilege in mind. If a user only needs to read specific files, the user should not have write access to those files, directories, or shares.

- Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.

- Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.

- Consider disabling Remote Desktop protocol (RDP) if it is not being used.

- Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.

- Execute operating system environments or specific programs in a virtualized environment.

- Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.[6]

53. To prevent and detect ransomware attacks, including the ransomware attack that resulted in the Data Breach, Defendant could and should have implemented, as recommended by the United States Cybersecurity & Infrastructure Security Agency, the following measures:

- **Update and patch your computer.** Ensure your applications and operating systems (OSs) have been updated with the latest patches. Vulnerable applications and OSs are the target of most ransomware attacks. . . .

- **Use caution with links and when entering website addresses.** Be careful when clicking directly on links in emails, even if the sender appears to be someone you know. Attempt to independently verify website addresses (e.g., contact your organization's helpdesk, search the internet for the sender organization's website or the topic mentioned in the email). Pay attention to the website addresses you click on, as well as those you enter yourself. Malicious website addresses often appear almost identical to legitimate sites, often using a slight variation in spelling or a different domain (e.g., .com instead of .net). . . .

- **Open email attachments with caution.** Be wary of opening email attachments, even from senders you think you know, particularly when attachments are compressed files or ZIP files.

- **Keep your personal information safe.** Check a website's security to ensure the information you submit is encrypted before you provide it. . . .

- **Verify email senders.** If you are unsure whether or not an email is legitimate, try to verify the email's legitimacy by contacting the sender directly. Do not click on any links in the email. If possible, use a previous (legitimate) email to ensure the contact information you have for the sender is authentic before you contact them.

- **Inform yourself.** Keep yourself informed about recent cybersecurity threats and up to date on ransomware techniques. You can find information about known phishing attacks on the Anti-Phishing Working Group website. You may also want to sign up for CISA product notifications, which will alert you when a new Alert, Analysis Report, Bulletin, Current Activity, or Tip has been published.

[6] *Id.* at 3-4.

- **Use and maintain preventative software programs.** Install antivirus software, firewalls, and email filters—and keep them updated—to reduce malicious network traffic. . . .[7]

54. To prevent and detect ransomware attacks, including the ransomware attack that resulted in the Data Breach, Defendant could and should have implemented, as recommended by the Microsoft Threat Protection Intelligence Team, the following measures:

Secure internet-facing assets
- Apply latest security updates
- Use threat and vulnerability management
- Perform regular audit; Remove privilege credentials

Thoroughly investigate and remediate alerts
- Prioritize and treat commodity malware infections as potential full comprise

Include IT Pros in security discussions
- Ensure collaboration among [security operations], [security admins], and [information technology] admins to configure servers and other endpoints securely

Build credential hygiene
- Use [multifactor authentication] or [network level authentication] and use strong, randomized, just-in-time local admin passwords
- Apply principle of least-privilege

Monitor for adversarial activities
- Hunt for brute force attempts
- Monitor for cleanup of Event logs
- Analyze logon events

Harden infrastructure
- Use Windows Defender Firewall
- Enable tamper protection
- Enable cloud-delivered protection
- Turn on attack surface reduction rules and [Antimalware Scan Interface] for Office [Visual Basic for Applications].[8]

---

[7] *See* Security Tip (ST19-001) Protecting Against Ransomware (original release date Apr. 11, 2019), *available at* https://www.cisa.gov/news-events/news/protecting-against-ransomware (last visited July 17, 2023).

[8] *See* Human-operated ransomware attacks: A preventable disaster (Mar 5, 2020), *available at* https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/ (last visited July 17, 2023).

55. Given that Defendant was storing the PII/PHI of other individuals, Defendant could and should have implemented all of the above measures to prevent and detect ransomware attacks.

56. The occurrence of the Data Breach indicates that Defendant failed to adequately implement one or more of the above measures to prevent ransomware attacks, resulting in the Data Breach and the exposure of the PII/PHI of Plaintiff and Class Members.

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

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

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

60. Defendant disregarded the rights of Plaintiff and Class Members by intentionally, willfully, recklessly, and/or negligently failing to take and implement adequate and reasonable measures to ensure that the PII/PHI 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 a result, the Plaintiff's and Class Members' PII/PHI was compromised through disclosure to an unknown and unauthorized criminal third party.

61. Upon information and belief, Defendant breached its duties and obligations in one or more of the following ways: (1) failing to design, implement, monitor, and maintain reasonable network safeguards against foreseeable threats; (2) failing to design, implement, and maintain reasonable data retention policies; (3) failing to adequately train staff on data security; (4) failing to comply with industry-standard data security practices; (5) failing to warn Plaintiff and Class Members of Defendant's inadequate data security practices; (6) failing to encrypt or adequately encrypt the PII/PHI; (7) failing to recognize or detect that its network had been compromised and accessed in a timely manner to mitigate the harm; (8) failing to utilize widely available software able to detect and prevent this type of attack; and (9) otherwise failing to secure the hardware using reasonable and effective data security procedures free of foreseeable vulnerabilities and data security incidents

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

Value of PII/PHI

63. The PII/PHI 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.[9] Experian reports that a stolen credit or

[9] *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 July 17, 2023).

debit card number can sell for $5 to $110 on the dark web.[10] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[11]

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

65. 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]

66. 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.

67. One such example of criminals using PII/PHI for profit is the development of "Fullz" packages.

68. Cyber-criminals can cross-reference two sources of PII/PHI to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree

---

[10] *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 July17, 2023).

[11] *In the Dark*, VPNOverview, 2019, *available at*: https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last accessed July 17, 2023).

[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 July 17, 2023).

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 PII/PHI from the Data Breach can easily be used to link and identify it to Plaintiff's and the 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 PII/PHI 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.

70. That is exactly what is happening to Plaintiff and members of the 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 PII/PHI is being misused, and that such misuse is fairly traceable to the Data Breach.

71. Theft of PHI, in particular, is gravely serious: "[a] thief may use your name or health insurance numbers to see a doctor, get prescription drugs, file claims with your insurance provider, or get other care. If the thief's health information is mixed with yours, your treatment, insurance and payment records, and credit report may be affected."[13]

72. Drug manufacturers, medical device manufacturers, pharmacies, hospitals, and other healthcare service providers often purchase PHI on the black market for the purpose of target marketing their products and services to the physical maladies of the data breach victims themselves. Insurance companies purchase and use wrongfully disclosed PHI to adjust their insureds' medical insurance premiums.

73. Healthcare data record may be valued at up to $250 per record on the black

[13] *See* Federal Trade Commission, *Medical Identity Theft*, http://www.consumer.ftc.gov/articles/0171-medical-identity-theft (last visited March 18, 2024).

market, compared to $5.40 for the next highest value record (a payment card).[14]

74. Because of the value of its collected and stored data, the medical industry has experienced disproportionally higher numbers of data theft events than other industries.

75. For this reason, Defendant knew or should have known about these dangers and strengthened its data and email handling systems accordingly. Defendant was on notice of the substantial and foreseeable risk of harm from a data breach, yet Defendant failed to properly prepare for that risk.

Defendant is a HIPAA Covered Entity

76. Defendant is a HIPAA covered entity that provides healthcare and medical services. As a regular and necessary part of its business, Defendant collects and custodies the highly sensitive PII/PHI of its patients and clients' patients. Defendant is required under federal and state law to maintain the strictest confidentiality of the patient's PII/PHI that it requires, receives, and collects, and Defendant is further required to maintain sufficient safeguards to protect that Private Information from being accessed by unauthorized third parties.

77. As a Defendant covered entity, Defendant is required to ensure that it will implement adequate safeguards to prevent unauthorized use or disclosure of PII/PHI, including by implementing requirements of the HIPAA Security Rule and to report any unauthorized use or disclosure of PII/PHI, including incidents that constitute breaches of unsecured PHI as in the case of the Data Breach complained of herein.

78. Due to the nature of Defendant's business, which includes providing a range of medical services, Defendant would be unable to engage in its regular business activities without

[14] Impravata, *Hackers, breaches, and the value of healthcare data,* (Jun. 30, 2021), https://www.imprivata.com/blog/healthcare-data-new-prize-hackers#:~:text=Often%20these%20attacks%20see%20hundreds,record%20(a%20payment%20card) (last visited March 18, 2024).

collecting and aggregating PII/PHI that it knows and understands to be sensitive and confidential.

79. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' PII/PHI, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiff's and Class Members' PII/PHI from unauthorized disclosure.

80. Plaintiff and Class Members are current or former patients and/or customers of Defendant whose PII/PHI was maintained by Defendant, or who received health-related or other services from Defendant, and directly or indirectly entrusted Defendant with their PII/PHI.

81. Plaintiff and the Class Members relied on Defendant to implement and follow adequate data security policies and protocols, to keep their PII/PHI confidential and securely maintained, to use such PII/PHI solely for business and health care purposes, and to prevent the unauthorized disclosures of the PII/PHI. Plaintiff and Class Members reasonably expected that Defendant would safeguard and keep their PII/PHI confidential.

82. As described throughout this Complaint, Defendant did not reasonably protect, secure, or store Plaintiff's and Class Members' PII/PHI prior to, during, or after the Data Breach, but rather, enacted unreasonable data security measures that it knew or should have known were insufficient to reasonably protect the highly sensitive information Defendant maintained. Consequently, cybercriminals circumvented Defendant's security measures, resulting in a significant data breach.

83. As a HIPAA covered entity that collects, creates, and maintains significant volumes of PII/PHI, the targeted attack was a foreseeable risk of which Defendant was aware and knew it had a duty to guard against. It is well-known that healthcare providers such as Defendant, which collect and store the confidential and sensitive PII/PHI of thousands of individuals, are frequently

targeted by cyberattacks. Further, cyberattacks are highly preventable through the implementation of reasonable and adequate cybersecurity safeguards, including proper employee cybersecurity training.

Defendant's Conduct Violates HIPAA Obligations to Safeguard Private Information

84. Defendant is a covered entity under HIPAA (45 C.F.R. § 160.102) and is required to comply with the HIPAA Privacy Rule and Security Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and E ("Standards for Privacy of Individually Identifiable Health Information"), and Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C.

85. HIPAA requires covered entities to protect against reasonably anticipated threats to the security of sensitive patient health information.

86. Defendant is subject to the rules and regulations for safeguarding electronic forms of medical information pursuant to the Health Information Technology Act ("HITECH").[5] *See* 42 U.S.C. §17921, 45 C.F.R. § 160.103.

87. HIPAA's Privacy Rule or *Standards for Privacy of Individually Identifiable Health Information* establishes national standards for the protection of health information that is kept or transferred in electronic form.

88. Covered entities must implement safeguards to ensure the confidentiality, integrity, and availability of PHI. Safeguards must include physical, technical, and administrative components.

89. The HIPAA Breach Notification Rule, 45 C.F.R. §§ 164.400–414, also requires Defendant to provide notice of the Data Breach to each affected individual "without unreasonable

delay and *in no case later than 60 days following discovery of the breach.*"[15]

90. Title II of HIPAA contains what are known as the Administrative Simplification provisions. 42 U.S.C. §§ 1301, *et seq.* These provisions require, among other things, that the Department of Health and Human Services ("HHS") create rules to streamline the standards for handling PII like the data Defendant left unguarded. The HHS subsequently promulgated multiple regulations under authority of the Administrative Simplification provisions of HIPAA. These rules include 45 C.F.R. § 164.306(a)(1-4); 45 C.F.R. § 164.312(a)(1); 45 C.F.R. § 164.308(a)(1)(i); 45 C.F.R. § 164.308(a)(1)(ii)(D), and 45 C.F.R. § 164.530(b).

91. A Data Breach, such as the one Defendant experienced, is considered a breach under the HIPAA Rules because there is an access of PHI not permitted under the HIPAA Privacy Rule. A breach under the HIPAA Rules is defined as:

> "...the acquisition, access, use, or disclosure of PHI in a manner not permitted under the [HIPAA Privacy Rule] which compromises the security or privacy of the PHI." *See* 45 C.F.R. 164.40.

92. 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

93. As shown above, experts studying cybersecurity routinely identify healthcare providers and partners as being particularly vulnerable to cyberattacks because of the value of the Private Information which they collect and maintain.

94. Several best practices have been identified that at a minimum should be implemented by healthcare providers like Defendant, including but not limited to; educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-

[15] https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html (last visited March 18, 2024).

malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data; and limiting which employees can access sensitive data.

95. Other best cybersecurity practices that are standard in the healthcare industry 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.

96. 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.

97. These foregoing frameworks are existing and applicable industry standards in the healthcare industry, and Defendant failed to comply with these accepted standards, thereby opening the door to the cyber incident and causing the data breach.

Defendant Fails to Adhere to FTC Guidelines

98. 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 PII/PHI.

99. The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[16] 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."[17]

100. 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 they keep;

b. Properly dispose of PII 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.

101. 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.

102. 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

[16] 17 C.F.R. § 248.201 (2013).
[17] *Id.*

on the network; and verify that third-party service providers have implemented reasonable security measures.

103. 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 ("FTC Act"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

104. Defendant's negligence and failure to employ reasonable and appropriate measures to protect against unauthorized access to Plaintiff and the Class's PII/PHI constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

Plaintiff's Experience

105. Plaintiff was a patient at Ortho RI.

106. After the Data Breach, Plaintiff began seeing unauthorized use of her bank card. As such, Plaintiff reasonably believes that her Private Information was compromised in the Data Breach.

107. As a result of the Data Breach, Plaintiff's sensitive information may have been accessed and/or acquired by an unauthorized actor. The confidentiality of Plaintiff's sensitive information has been irreparably harmed. For the rests of her life, Plaintiff will have to worry about when and how her sensitive information may be shared or used to her detriment

108. As a result of the Data Breach, Plaintiff spent time dealing with the consequences of the Data Breach, which includes times spent verifying the legitimacy of the Notice of Data Breach and self-monitoring her accounts. This time has been lost forever and cannot be recaptured.

109. Additionally, Plaintiff is very careful about not sharing her sensitive PII. She has never knowingly transmitted unencrypted sensitive PII/PHI over the internet or any other unsecured source.

110. Plaintiff stores any documents containing her sensitive PII/PHI in safe and secure locations or destroys the documents. Moreover, she diligently chooses unique usernames and passwords for her various online accounts.

111. Plaintiff suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and experiences fear and anxiety and increased concern for the loss of her privacy.

112. Plaintiff has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from her PII, especially her Social Security number, being placed in the hands of unauthorized third parties and possibly criminals.

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

Plaintiff's and the Class Members' Injuries

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

115. Defendant negligently disclosed the PII/PHI of Plaintiff and the Class for criminals to use in the conduct of criminal activity. Specifically, Defendant opened up, disclosed, and exposed the PII/PHI 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 PII/PHI.

116. Defendant was, or should have been, fully aware of the unique type and the significant volume of data contained in Defendant's database, 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.

117. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the PII/PHI 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.

118. The injuries to Plaintiff and Class Members are directly and proximately caused by Defendant's negligence and failure to implement or maintain adequate data security measures for the PII/PHI of Plaintiff and Class Members.

119. As a result of Defendant's negligence and failure to prevent the Data Breach, Plaintiff and the 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. Identity theft;

b. Misuse of their PII;

c. The loss of the opportunity to control how their PII is used;

d. The diminution in value of their PII;

e. The compromise and continuing publication of their PII;

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

g. Loss 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 spend researching how to prevent, detect, contest, and recover form identity theft and fraud;

h. Delay in receipt of tax refund monies;

i. Unauthorized use of stolen PII; and

j. The continued risk to their PII, 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 PII in their possession.

Plaintiff's and the Class Members' PII is Available on the Dark Web

120. Upon information and belief, the unauthorized third-party cybercriminals gained access to Plaintiff's and Class Members' PII/PHI with the intent of engaging in misuse of the PII/PHI, including marketing and selling Plaintiff's and Class Members' PII/PHI.

121. Upon information and believe, the unencrypted Private Information of Plaintiff and Class Members is for sale on the dark web because that is the *modus operandi* of hackers.

122. Plaintiff has already seen fraud on her financial account. Plaintiff did not have any issues with this financial account prior to the Data Breach. As such, Plaintiff reasonably believes that her information was sold on the Dark Web, resulting in the fraudulent misuse.

123. The dark web is an unindexed layer of the internet that requires special software or

authentication to access.[18] Criminals in particular favor the dark web as it offers a degree of anonymity to visitors and website publishers. Unlike the traditional or "surface" web, dark web users need to know the web address of the website they wish to visit in advance. For example, on the surface web, the CIA's web address is cia.gov, but on the dark web the CIA's web address is ciadotgov4sjwlzihbbgxnqg3xiyrg7so2r2o3lt5wz5ypk4sxyjstad.onion.[19] This prevents dark web marketplaces from being easily monitored by authorities or accessed by those not in the know.

124. A sophisticated black market exists on the dark web where criminals can buy or sell malware, firearms, drugs, and frequently, PHI and PII like the Private Information at issue here.[20] The digital character of PII/PHI stolen in data breaches lends itself to dark web transactions because it is immediately transmissible over the internet and the buyer and seller can retain their anonymity. The sale of a firearm or drugs on the other hand requires a physical delivery address. Nefarious actors can readily purchase usernames and passwords for online streaming services, stolen financial information and account login credentials, and Social Security numbers, dates of birth, and medical information.[21] As Microsoft warns "[t]he anonymity of the dark web lends itself well to those who would seek to do financial harm to others."[22]

Plaintiff and the Class Members Have Experienced Misuse

125. As a result of the Data Breach, the unencrypted and detailed PII/PHI of Plaintiff and the Class Members has fall into the hands of companies that will use it for targeted marketing

---

[18] *What Is the dark web?*, Experian, available at https://www.experian.com/blogs/ask-experian/what-is-the-dark-web/.
[19] *Id.*
[20] *What is the dark web?* – Microsoft 365, available at https://www.microsoft.com/en-us/microsoft-365-life-hacks/privacy-and-safety/what-is-the-dark-web.
[21] *Id.; What Is the dark web?*, Experian, available at https://www.experian.com/blogs/ask-experian/what-is-the-dark-web/.
[22] *What is the dark web?* – Microsoft 365, available at https://www.microsoft.com/en-us/microsoft-365-life-hacks/privacy-and-safety/what-is-the-dark-web.

without the approval of Plaintiff and Class Members, as seen by the increase in spam calls and emails. Unauthorized actors can easily access and misuse Plaintiff's and Class Members' PII/PHI due to the Data Breach. Plaintiff has already experienced misuse of her PII/PHI as a result of the Data Breach.

126. The link between a data breach and the risk of identity theft is simple and well established. Criminals acquire and steal PII/PHI to monetize the information. Criminals monetize the data by selling the stolen information on the black market to other criminals who then utilize the information to commit a variety of identity theft related crimes discussed herein.

127. Because a person's identity is akin to a puzzle with multiple data points, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity--or track the victim to attempt other hacking crimes against the individual to obtain more data to perfect a crime.

128. For example, armed with just a name and Social Security number, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or financial account information. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate and trick individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails. Data Breaches can be the starting point for these additional targeted attacks on the victim.

129. Moreover, the existence and prevalence of "Fullz" packages means that the PII/PHI stolen from the data breach can easily be linked to the unregulated data (like phone numbers and emails) of Plaintiff and the other Class Members.

130. Thus, even if certain information (such as emails or telephone numbers) was not stolen in the data breach, criminals can still easily create a comprehensive "Fullz" package.

131. Then, this comprehensive dossier can be sold—and then resold in perpetuity—to crooked operators and other criminals (like illegal and scam telemarketers).

132. Social Security numbers, for example, are among the worst kind of personal information to have stolen because they may be put to numerous serious 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. 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.[23]

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

134. Even then, new Social Security number may not be effective, as "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that

[23] Social Security Administration, *Identity Theft and Your Social Security Number*, available at: https://www.ssa.gov/pubs/EN-05-10064.pdf.

old bad information is quickly inherited into the new Social Security number."[24]

135. Identity thieves can also use Social Security numbers to obtain a driver's license or official identification card in the victim's name but with the thief's picture; use the victim's name and Social Security number to obtain government benefits; or file a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's Social Security number, rent a house or receive medical services in the victim's name, and may even give the victim's personal information to police during an arrest resulting in an arrest warrant issued in the victim's name. And the Social Security Administration has warned that identity thieves can use an individual's Social Security number to apply for credit lines.[25]

136. Victims of identity theft can suffer from both direct and indirect financial losses. According to a research study published by the Department of Justice,

> A direct financial loss is the monetary amount the offender obtained from misusing the victim's account or personal information, including the estimated value of goods, services, or cash obtained. It includes both out-of-pocket loss and any losses that were reimbursed to the victim. An indirect loss includes any other monetary cost caused by the identity theft, such as legal fees, bounced checks, and other miscellaneous expenses that are not reimbursed (e.g., postage, phone calls, or notary fees). All indirect losses are included in the calculation of out-of-pocket loss.[26]

137. According to the FBI's Internet Crime Complaint Center (IC3) 2019 Internet Crime Report, Internet-enabled crimes reached their highest number of complaints and dollar losses that

---

[24] Brian Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft (last visited Aug. 23, 2024).

[25] *Identity Theft and Your Social Security Number*, Social Security Administration, 1 (2018), available at https://www.ssa.gov/pubs/EN-05-10064.pdf.

[26] Erika Harrell, *Bureau of Just. Stat.*, U.S. DEP'T OF JUST., NCJ 256085, *Victims of Identity Theft*, 2018 I (2020) https://bjs.ojp.gov/content/pub/pdf/vit18.pdf (last accessed Jan. 23, 2024).

year, resulting in more than $3.5 billion in losses to individuals and business victims.[27]

138. Further, according to the same report, "rapid reporting can help law enforcement stop fraudulent transactions before a victim loses the money for good."[28] Yet, Defendants failed to rapidly report to Plaintiff and Class Members that their Private Information was stolen.

Plaintiff's and the Class Members' Lost Time

139. Plaintiff and the Class Members have also spent considerable time and will continue to spend considerable time to protect themselves and keep their identities and personal property protected.

140. . Time is a compensable and valuable resource in the United States. According to the U.S. Bureau of Labor Statistics, 55.5% of U.S.-based workers are compensated on an hourly basis, while the other 44.5% are salaried.[29]

141. According to the U.S. Bureau of Labor Statistics' 2018 American Time Use Survey, American adults have only 36 to 40 hours of "leisure time" outside of work per week; leisure time is defined as time not occupied with work or chores and is "the time equivalent of 'disposable income.'"[30] Usually, this time can be spent at the option and choice of the consumer, however, having been notified of the Data Breach, consumers now have to spend hours of their leisure time

---

[27] *See* https://www.fbi.gov/news/stories/2019-internet-crime-report-released-021120.
[28] *Id.*
[29] *Characteristics of minimum wage workers, 2020*, U.S. BUREAU OF LABOR STATISTICS https://www.bls.gov/opub/reports/minimum-wage/2020/home.htm#:~:text=%20In%202020%2C%2073.3%20million%20workers,wage%20of%20%247.25%20 per%20hour (last accessed March 18, 2024); *Average Weekly Wage Data*, U.S. BUREAU OF LABOR STATISTICS, *Average Weekly Wage Data*, https://www.bls.gov/news.release/pdf/wkyeng.pdf (last accessed May 9 2024) (finding that on average, private-sector workers make $1,145 per 40-hour work week.).
[30] Cory Stieg, *You're spending your free time wrong — here's what to do to be happier and more successful*, CNBC https://www.cnbc.com/2019/11/06/how-successful-people-spend-leisure-time-james-wallman.html (Nov. 6, 2019) (last accessed May 9, 2024).

self-monitoring their accounts, communicating with financial institutions and government entities, and placing other prophylactic measures in place to attempt to protect themselves.

142. Plaintiff and Class Members are now deprived of the choice as to how to spend their valuable free hours and seek renumeration for the loss of valuable time as another element of damages.

Plaintiff's and the Class Members Heightened Risk of Identity Theft and Ongoing Injuries

143. Cyberattacks and data breaches at healthcare companies and partner companies like Defendant are especially problematic because they can negatively impact the overall daily lives of individuals affected by the attack.

144. Researchers have found that among medical service providers that experience a data security incident, the death rate among patients increased in the months and years after the attack.[31]

145. Researchers have further found that at medical service providers that experienced a data security incident, the incident was associated with deterioration in timeliness and patient outcomes, generally.[32]

146. The United States Government Accountability Office released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft face "substantial costs and time to repair the damage to their good name and credit record."[33]

147. That is because any victim of a data breach is exposed to serious ramifications

---

[31] *See* Nsikan Akpan, *Ransomware and Data Breaches Linked to Uptick in Fatal Heart Attacks*, PBS (Oct. 24, 2019), https://www.pbs.org/newshour/science/ransomware-and-other-data-breaches-linked-to-uptick-in-fatal-heart-attacks (last visited March 18, 2024).

[32] *See* Sung J. Choi et al., *Data Breach Remediation Efforts and Their Implications for Hospital Quality*, 54 Health Services Research 971, 971-980 (2019), available at https://onlinelibrary.wiley.com/doi/full/10.1111/1475-6773.13203.

[33] *See* U.S. Gov't Accounting Office, GAO-07-737, Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown (2007), available at https://www.gao.gov/new.items/d07737.pdf (last visited March 18, 2024).

regardless of the nature of the data. Indeed, the reason criminals steal personally identifiable information is to monetize it by selling the spoils of their cyberattacks on the black market to identity thieves who desire to extort and harass victims, take over victims' identities in order to engage in illegal financial transactions under the victims' names. Because a person's identity is akin to a puzzle, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity, or otherwise harass or track the victim. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails.

148. The FTC recommends that identity theft victims take several steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for seven years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[34]

149. Identity thieves use stolen personal information such as Social Security numbers for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.

150. Identity thieves can also use Social Security numbers to obtain a driver's license or official identification card in the victim's name but with the thief's picture; use the victim's name

[34] *See IdentityTheft.gov*, Federal Trade Commission, https://www.identitytheft.gov/Steps (last visited March 18, 2024).

and Social Security number to obtain government benefits; or file a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's Social Security number, rent a house or receive medical services in the victim's name, and may even give the victim's personal information to police during an arrest resulting in an arrest warrant being issued in the victim's name.

151. Moreover, theft of PII/PHI is also gravely serious because PII/PHI is an extremely valuable property right.[35]

152. Its value is axiomatic, considering the value of "big data" in corporate America and the fact that the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that PII/PHI has considerable market value.

153. Additional fraudulent activity resulting from the Data Breach may not come to light for years.

154. There may be a time lag between when harm occurs versus when it is discovered, and also between when PII/PHI 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, 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.[36]

---

[35] *See, e.g.*, John T. Soma, et al, *Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets*, 15 Rich. J.L. & Tech. 11, at *3–4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

[36] *Report to Congressional Requesters*, GAO, at 29 (June 2007), *available at:* https://www.gao.gov/assets/gao-07-737.pdf (last accessed July 17, 2023).

155. As a result of the Data Breach, Cybercriminals also have sufficient information to pose as legitimate persons and gain more information from Plaintiff and the Class Members, putting Plaintiff and the Class Members at a continuing risk of identity theft.

156. Victims of identity theft also often suffer embarrassment, blackmail, or harassment in person or online, and/or experience financial losses resulting from fraudulently opened accounts or misuse of existing accounts.

157. In addition to out-of-pocket expenses that can exceed thousands of dollars and the emotional toll identity theft can take, some victims must spend a considerable time repairing the damage caused by the theft of their Private Information. Victims of new account identity theft will likely have to spend time correcting fraudulent information in their credit reports and continuously monitor their reports for future inaccuracies, close existing bank/credit accounts, open new ones, and dispute charges with creditors.

158. Further complicating the issues faced by victims of identity theft, data thieves may wait years before attempting to use the stolen PII/PHI. To protect themselves, Plaintiff and Class Members will need to remain vigilant for years or even decades to come.

159. Defendant's negligence and 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 PII/PHI and take other necessary steps to mitigate the harm caused by the Data Breach.

160. 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/PHI.

Future Cost of Credit and Identity Theft Monitoring is Reasonable and Necessary

161. To date, Defendant has offered Plaintiff and some Class Members an inadequate amount of credit monitoring services. The offered service is inadequate to protect Plaintiff and Class Members from the threats they face for years to come, particularly in light of the PII/PHI at issue here.

162. Given the type of targeted attack in this case and sophisticated criminal activity, the type of PII/PHI, and the *modus operandi* of cybercriminals, there is a strong probability that entire batches of stolen information have been placed, or will be placed, on the black market/dark web for sale and purchase by criminals intending to utilize the PII/PHI for identity theft crimes—*e.g.*, opening bank accounts in the victims' names to make purchases or to launder money, filing false tax returns, taking out loans or lines of credit, or filing false unemployment claims.

163. Such fraud may go undetected until debt collection calls commence months, or even years, later. An individual may not know that her or her Social Security number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

164. Furthermore, the information accessed and disseminated in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach, where victims can easily cancel or close credit and debit card accounts.[37] The information disclosed in this Data Breach is impossible to "close" and difficult, if not impossible, to change (such as Social Security numbers).

165. Consequently, Plaintiff and Class Members are at a present and ongoing risk of

[37] *See* Jesse Damiani, *Your Social Security Number Costs $4 On The dark web, New Report Finds*, FORBES (Mar. 25, 2020), https://www.forbes.com/sites/jessedamiani/2020/03/25/your-social-security-number-costs-4-on-the-dark-web-new-report-finds/?sh=6a44b6d513f1.

fraud and identity theft for many years into the future, if not forever.

166. The retail cost of credit monitoring and identity theft monitoring can cost $200 or more a year per Class Member. This is a reasonable and necessary cost to protect Class Members from the risk of identity theft that arose from Defendant's Data Breach. This is a future cost for a minimum of five years that Plaintiff and Class Members would not need to bear but for Defendant's failure to safeguard their PII/PHI.

V. CLASS ACTION ALLEGATIONS

167. Plaintiff brings this nationwide class action on behalf of herself and on behalf of all others similarly situated pursuant to R.I. Super. Ct. R. Civ. P. 23.

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

> All individuals whose PII/PHI may have been accessed and/or acquired in the ransomware attack that is the subject of the Notice of Data Breach.

169. Excluded from the Classes 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.

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

171. **Numerosity:** The Class is so numerous that joinder of all members is impracticable. Upon information and belief, hundreds of individuals had their information impacted by the Data Breach.

172. **Commonality:** 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/PHI of Plaintiff and Class Members;

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

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

d. Whether Defendant failed to adequately safeguard the PII/PHI 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/PHI had been compromised;

g. Whether Defendant violated the law by failing to promptly notify Plaintiff and Class Members that their PII/PHI 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 practice by failing to safeguard the PII/PHI 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.

173. **Typicality:** Plaintiff's claims are typical of those of other Class Members because all had their PII/PHI compromised as a result of the Data Breach, due to Defendant's misfeasance.

174. **Policies Generally Applicable to the Class:** This class action is also appropriate for certification because Defendant has acted or refused to act on grounds generally applicable to the Class, 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 Class 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 Class as a whole, not on facts or law applicable only to Plaintiff.

175. **Adequacy:** Plaintiff will fairly and adequately represent and protect the interests of Class Members in that they have no disabling conflicts of interest that would be antagonistic to those of the other Members of the Class. Plaintiff seeks no relief that is antagonistic or adverse to the Members of the Class and the infringement of the rights and the damages they have 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.

176. **Superiority and Manageability:** 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.

177. 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 Class 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.

178. 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.

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

180. Unless a Class-wide injunction is issued, Defendant may continue in its failure to properly secure the PII/PHI 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.

181. 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.

182. Likewise, particular issues 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 Defendant adequately and accurately informed Plaintiff and Class

Members that their PII/PHI had been compromised;

e. 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;

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

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

VI. CAUSES OF ACTION

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

183. Plaintiff incorporates by reference all allegations of the preceding paragraphs as though fully set forth herein.

184. Defendant solicited, gathered, and stored the PII/PHI Plaintiff and the Class as part of the operation of its business.

185. Upon accepting and storing the PII/PHI of Plaintiff and Class Members, Defendant undertook and owed a duty to Plaintiff and Class Members to exercise reasonable care to secure and safeguard that information and to use secure methods to do so.

186. Defendant had full knowledge of the sensitivity of the PII, the types of harm that Plaintiff and Class members could and would suffer if the PII/PHI was wrongfully disclosed, and the importance of adequate security.

187. Plaintiff and Class members were the foreseeable victims of any inadequate safety and security practices. Plaintiff and the Class members had no ability to protect their PII/PHI that

was in Defendant's possession. As such, a special relationship existed between Defendant and Plaintiff and the Class.

188. Defendant was well aware of the fact that cyber criminals routinely target large corporations through cyberattacks in an attempt to steal sensitive PII.

189. Defendant owed Plaintiff and the Class members a common law duty to use reasonable care to avoid causing foreseeable risk of harm to Plaintiff and the Class when obtaining, storing, using, and managing personal information, including taking action to reasonably safeguard such data.

190. Defendant's duty extended to protecting Plaintiff and the Class from the risk of foreseeable criminal conduct of third parties, which has been recognized in situations where the actor's own conduct or misconduct exposes another to the risk or defeats protections put in place to guard against the risk, or where the parties are in a special relationship. *See* Restatement (Second) of Torts § 302B. Numerous courts and legislatures also have recognized the existence of a specific duty to reasonably safeguard personal information.

191. Defendant had duties to protect and safeguard the PII/PHI of Plaintiff and the Class from being vulnerable to cyberattacks by taking common-sense precautions when dealing with sensitive PII. Additional duties that Defendant owed Plaintiff and the Class include:

a. To exercise reasonable care in designing, implementing, maintaining, monitoring, and testing Defendant's networks, systems, protocols, policies, procedures and practices to ensure that Plaintiff's and Class Members' PII/PHI was adequately secured from impermissible access, viewing, release, disclosure, and publication;

b. To protect Plaintiff's and Class Members' PII/PHI in its possession by using reasonable and adequate security procedures and systems;

c. To implement processes to quickly detect a data breach, security incident, or intrusion involving their networks and servers; and

d. To promptly notify Plaintiff and Class Members of any data breach, security incident, or intrusion that affected or may have affected their PII.

192. Defendant was the only one who could ensure that its systems and protocols were sufficient to protect the PII/PHI that Plaintiff and the Class had entrusted to it.

193. Defendant breached its duties of care by failing to adequately protect Plaintiff's and Class Members' PII. Defendant breached its duties by, among other things:

a. Failing to exercise reasonable care in obtaining, retaining securing, safeguarding, deleting, and protecting the PII/PHI in its possession;

b. Failing to protect the PII/PHI in its possession using reasonable and adequate security procedures and systems;

c. Failing to adequately train its employees to not store PII/PHI longer than absolutely necessary;

d. Failing to consistently enforce security policies aimed at protecting Plaintiff's and the Class's PII; and

e. Failing to implement processes to quickly detect data breaches, security incidents, or intrusions.

194. Defendant's willful failure to abide by these duties was wrongful, reckless, and grossly negligent in light of the foreseeable risks and known threats.

195. As a proximate and foreseeable result of Defendant's negligent and/or grossly negligent conduct, Plaintiff and the Class have suffered damages and are at imminent risk of additional harms and damages.

196. Through Defendant's acts and omissions described herein, including but not limited to Defendant's failure to protect the PII/PHI of Plaintiff and Class Members from being stolen and misused, Defendant unlawfully breached its duty to use reasonable care to adequately protect and secure the PII/PHI of Plaintiff and Class Members while it was within Defendant's possession and control.

197. As a result of the Data Breach, Plaintiff and Class Members have spent time, effort, and money to mitigate the actual and potential impact of the Data Breach on their lives, including but not limited to, closely reviewing and monitoring bank accounts, credit reports, and statements sent from providers and their insurance companies and the payment for credit monitoring and identity theft prevention services.

198. Defendant's wrongful actions, inactions, and omissions constituted (and continue to constitute) common law negligence.

199. The damages Plaintiff and the Class have suffered and will suffer were and are the direct and proximate result of Defendant's negligent and/or grossly negligent conduct.

COUNT II – NEGLIGENCE *PER SE*
(On Behalf of Plaintiff and the Class)

200. Plaintiff incorporates by reference all allegations of the preceding paragraphs as though fully set forth herein.

201. In addition to its duties under common law, Defendant had additional duties imposed by statute and regulations, including the duties the FTC Act, HIPAA, and other state and federal statutes. The harms which occurred as a result of Defendant's failure to observe these

duties, including the loss of privacy and significant risk of identity theft, are the types of harm that these statutes and their regulations were intended to prevent.

202. 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 and Class Members' PII.

203. 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 PII. The FTC publications and orders also form part of the basis of Defendant's duty in this regard.

204. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect consumers PII/PHI and not complying with applicable industry standards, as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of PII/PHI it obtained and stored, and the foreseeable consequences of a data breach including, specifically, the damages that would result to Plaintiff and Class Members.

205. Defendant's violation of Section 5 of the FTC Act constitutes negligence *per se* as Defendant's violation of the FTC Act establishes the duty and breach elements of negligence.

206. Plaintiff and Class Members are within the class of persons that the FTC Act was intended to protect.

207. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result 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.

208. But for Defendant's wrongful and negligent breach of its duties owed to Plaintiff and Class Members, Plaintiff and Class Members would not have been injured.

209. The injury and harm suffered by Plaintiff and Class Members was the reasonably foreseeable result of Defendant's breach of its duties. Defendant knew or should have known that it was failing to meet their duties, and that Defendant's breach would cause Plaintiff and Class Members to experience the foreseeable harms associated with the exposure of their PII.

210. As a direct and proximate result of Defendant's negligent conduct, Plaintiff and Class Members have suffered injury and are entitled to compensatory, consequential, and punitive damages in an amount to be proven at trial.

COUNT III – INVASION OF PRIVACY
(On Behalf of Plaintiff and the Class)

211. Plaintiff incorporates by reference all allegations of the preceding paragraphs as though fully set forth herein.

212. Plaintiff and Class Members had a legitimate expectation of privacy regarding their PII/PHI and were accordingly entitled to the protection of this information against disclosure to unauthorized third parties.

213. Defendant owed a duty to Plaintiff and Class Member to keep their PII/PHI confidential.

214. Defendant affirmatively and recklessly disclosed Plaintiff and Class Members' PII/PHI to unauthorized third parties.

215. The unauthorized disclosure and/or acquisition (i.e., theft) by a third party of Plaintiff and Class Members' PII/PHI is highly offensive to a reasonable person.

216. Defendant's reckless and negligent failure to protect Plaintiff and Class Members' PII/PHI constitutes an intentional interference with Plaintiff and the Class Members' interest in

solitude or seclusion, either as to their person or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

217. In failing to protect Plaintiff and Class Members' PII, Defendant acted with a knowing state of mind when it permitted the Data Breach because it knew its information security practices were inadequate.

218. Because Defendant failed to properly safeguard Plaintiff and Class Members' PII, Defendant had notice and knew that its inadequate cybersecurity practices would cause injury to Plaintiff and the Class.

219. Defendant knowingly did not notify Plaintiff and Class Members in a timely fashion about the Data Breach.

220. As a proximate result of Defendant's acts and omissions, Plaintiff and the Class Members' private and sensitive PII/PHI was stolen by a third party and is now available for disclosure and redisclosure without authorization, causing Plaintiff and the Class to suffer damages.

221. Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiff and the Class since their PII/PHI are still maintained by Defendant with their inadequate cybersecurity system and policies.

222. Plaintiff and Class Members have no adequate remedy at law for the injuries relating to Defendant's continued possession of their sensitive and confidential records. A judgment for monetary damages will not end Defendant's inability to safeguard Plaintiff and the Class's PII.

223. Plaintiff, on behalf of herself and Class Members, seeks injunctive relief to enjoin Defendant from further intruding into the privacy and confidentiality of Plaintiff and Class

Members' PII.

224. Plaintiff, on behalf of herself and Class Members, seeks compensatory damages for Defendant's invasion of privacy, which includes the value of the privacy interest invaded by Defendant, the costs of future monitoring of their credit history for identity theft and fraud, plus prejudgment interest, and costs.

COUNT IV – BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiff and the Class)

225. Plaintiff incorporates by reference all allegations of the preceding paragraphs as though fully set forth herein.

226. By requiring Plaintiff and the Class Members PII/PHI to do business with receive medial services from Defendant, Defendant entered into an implied contract in which Defendant agreed to comply with its statutory and common law duties to protect Plaintiff and Class Members' PII. In return, Defendant provided goods to Plaintiff and the Class.

227. Based on this implicit understanding, Plaintiff and the Class accepted Defendant's offers and provided Defendant with their PII.

228. Plaintiff and Class members would not have provided their PII/PHI to Defendant had they known that Defendant would not safeguard their PII, as promised.

229. Plaintiff and Class members fully performed their obligations under the implied contracts with Defendant.

230. Defendant breached the implied contracts by failing to safeguard Plaintiff and Class Members' PII.

231. Defendant also breached the implied contracts when it engaged in acts and/or omissions that are declared unfair trade practices by the FTC. These acts and omissions included (i) representing, either expressly or impliedly, that it would maintain adequate data privacy and

security practices and procedures to safeguard the PII/PHI from unauthorized disclosures, releases, data breaches, and theft; (ii) omitting, suppressing, and concealing the material fact of the inadequacy of the privacy and security protections for the Class's PII; and (iii) failing to disclose to Plaintiff and the Class at the time they provided their PII/PHI that Defendant's data security system and protocols failed to meet applicable legal and industry standards.

232. The losses and damages Plaintiff and Class members sustained were the direct and proximate result of Defendant's breach of the implied contract with Plaintiff and Class Members.

COUNT V – BREACH OF CONFIDENCE
(On Behalf of Plaintiff and the Class)

233. Plaintiff incorporates by reference all allegations of the preceding paragraphs as though fully set forth herein.

234. Defendant was fully aware of the confidential nature of the PII/PHI of Plaintiff and Class Members that it was provided.

235. As alleged herein and above, Defendant's relationship with Plaintiff and the Class was governed by promises and expectations that Plaintiff and Class Members' PII/PHI would be collected, stored, and protected in confidence, and would not be accessed by, acquired by, appropriated by, disclosed to, encumbered by, exfiltrated by, released to, stolen by, used by, and/or viewed by unauthorized third parties.

236. Plaintiff and Class members provided their respective PII/PHI to Defendant with the explicit and implicit understandings that Defendant would protect and not permit the PII/PHI to be accessed by, acquired by, appropriated by, disclosed to, encumbered by, exfiltrated by, released to, stolen by, used by, and/or viewed by unauthorized third parties.

237. Plaintiff and Class Members provided their PII/PHI to Defendant with the explicit and implicit understandings that Defendant would take precautions to protect their PII/PHI from

unauthorized access, acquisition, appropriation, disclosure, encumbrance, exfiltration, release, theft, use, and/or viewing, such as following basic principles of protecting their networks and data systems.

238. Defendant voluntarily received, in confidence, Plaintiff and Class members' PII/PHI with the understanding that the PII/PHI would not be accessed by, acquired by, appropriated by, disclosed to, encumbered by, exfiltrated by, released to, stolen by, used by, and/or viewed by the public or any unauthorized third parties.

239. Due to Defendant's failure to prevent, detect, and avoid the Data Breach from occurring by, inter alia, not following best information security practices to secure Plaintiff and Class Members' PII, Plaintiff and Class Members' PII/PHI was accessed by, acquired by, appropriated by, disclosed to, encumbered by, exfiltrated by, released to, stolen by, used by, and/or viewed by unauthorized third parties beyond Plaintiff and Class Members' confidence, and without their express permission.

240. As a direct and proximate cause of Defendant's actions and/or omissions, Plaintiff and Class members have suffered damages as alleged herein.

241. But for Defendant's failure to maintain and protect Plaintiff and Class Members' PII/PHI in violation of the parties' understanding of confidence, their PII/PHI would not have been accessed by, acquired by, appropriated by, disclosed to, encumbered by, exfiltrated by, released to, stolen by, used by, and/or viewed by unauthorized third parties. Defendant's Data Breach was the direct and legal cause of the misuse of Plaintiff and Class members' PII, as well as the resulting damages.

242. The injury and harm Plaintiff and Class Members suffered and will continue to suffer was the reasonably foreseeable result of Defendant's unauthorized misuse of Plaintiff and

Class members' PII. Defendant knew its data systems and protocols for accepting and securing Plaintiff and Class Members' PII/PHI had security and other vulnerabilities that placed Plaintiff and Class members' PII/PHI in jeopardy.

243. As a direct and proximate result of Defendant's breaches of confidence, Plaintiff and Class members have suffered and will suffer injury, as alleged herein, including but not limited to (a) actual identity theft; (b) the compromise, publication, and/or theft of their PII; (c) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their PII; (d) 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 identity theft; (e) the continued risk to their PII, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fail to undertake appropriate and adequate measures to protect Class Members' PII/PHI in their continued possession; (f) future costs in terms of time, effort, and money that will be expended as result of the Data Breach for the remainder of the lives of Plaintiff and Class Members; and (g) the diminished value of Plaintiff and Class Members' PII.

COUNT VI – BREACH OF FIDUCIARY DUTY
(On Behalf of Plaintiff and the Class)

244. Plaintiff incorporates by reference all preceding factual allegations as though fully alleged herein.

245. A relationship existed between Plaintiff and Class Members and Defendant in which Plaintiff and the Class put their trust in Defendant to protect their PII. Defendant accepted this duty and obligation when it received Plaintiff and the Class Members' PII.

246. Plaintiff and the Class Members entrusted their PII/PHI to Defendant on the premise and with the understanding that Defendant would safeguard their information, use their PII/PHI for business purposes only, and refrain from disclosing their PII/PHI to unauthorized third parties.

247. Defendant knew or should have known that the failure to exercise due care in the collecting, storing, and using of individual's PII/PHI involved an unreasonable risk of harm to Plaintiff and the Class, including harm that foreseeably could occur through the criminal acts of a third party.

248. Defendant's fiduciary duty required it 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 Plaintiff and the Class's information in Defendant's possession was adequately secured and protected.

249. Defendant also had a fiduciary duty to have procedures in place to detect and prevent improper access and misuse of Plaintiff's and the Class's PII. Defendant's duty to use reasonable security measures arose as a result of the special relationship that existed between Defendant and Plaintiff and the Class. That special relationship arose because Defendant was entrusted with Plaintiff and the Class's PII.

250. Defendant breached its fiduciary duty that it owed Plaintiff and the Class by failing to case in good faith, fairness, and honesty; by failing to act with the highest and finest loyalty; and by failing to protect the PII/PHI of Plaintiff and the Class Members.

251. Defendant's breach of fiduciary duties was a legal cause of damages to Plaintiff and the Class.

252. But for Defendant's breach of fiduciary duty, the damage to Plaintiff and the Class would not have occurred, and the Data Breach contributed substantially to producing the damage to Plaintiff and the Class.

253. As a direct and proximate result of Defendant's breach of fiduciary duty, Plaintiff and the Class are entitled to actual, consequential, and nominal damages and injunctive relief, with amounts to be determined at trial.

COUNT VII – DECLARTORY JUDGMENT
(On Behalf of Plaintiff and the Class)

254. Plaintiff incorporates by reference all allegations of the preceding paragraphs as though fully set forth herein.

255. This Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Further, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal and state statutes described in this Complaint.

256. An actual controversy has arisen in the wake of the Data Breach regarding Plaintiff's and the Class's PII/PHI and whether Defendant is currently maintaining data security measures adequate to protect Plaintiff and the Class from further data breaches that compromise their PII. Plaintiff alleges that Defendant's data security measures remain inadequate. Defendant publicly denies these allegations. Furthermore, Plaintiff continues to suffer injury as a result of the compromise of her PII/PHI and remains at imminent risk that further compromises of their PII/PHI will occur in the future. It is unknown what specific measures and changes Defendant has undertaken in response to the Data Breach.

257. Plaintiff and the Class have an ongoing, actionable dispute arising out of Defendant's inadequate security measures, including (i) Defendant's failure to encrypt Plaintiff's

and the Class's PII, including Social Security numbers, while storing it in an Internet-accessible environment, and (ii) Defendant's failure to delete PII/PHI it has no reasonable need to maintain in an Internet-accessible environment, including the Social Security numbers of Plaintiff and the Class.

258. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. Defendant owes a legal duty to secure the PII/PHI of Plaintiff and the Class;

b. Defendant continues to breach this legal duty by failing to employ reasonable measures to secure consumers' PII; and

c. Defendant's ongoing breaches of its legal duty continue to cause Plaintiff and the Class harm.

259. This Court also should issue corresponding prospective injunctive relief requiring Defendant to employ adequate security protocols consistent with law and industry and government regulatory standards to protect consumers' PII. Specifically, this injunction should, among other things, direct Defendant to:

a. engage third party auditors, consistent with industry standards, to test its systems for weakness and upgrade any such weakness found;

b. audit, test, and train its data security personnel regarding any new or modified procedures and how to respond to a data breach;

c. regularly test its systems for security vulnerabilities, consistent with industry standards;

d. implement an education and training program for appropriate employees

regarding cybersecurity.

260. If an injunction is not issued, Plaintiff and Class Members will suffer irreparable injury, and lack an adequate legal remedy, in the event of another data breach at Defendant. The risk of another such breach is real, immediate, and substantial. If another breach at Defendant occurs, Plaintiff will not have an adequate remedy at law because many of the resulting injuries are not readily quantified and they will be forced to bring multiple lawsuits to rectify the same conduct.

261. The hardship to Plaintiff and Class Members if an injunction is not issued exceeds the hardship to Defendant if an injunction is issued. Plaintiff will likely be subjected to substantial identity theft and other damage. On the other hand, the cost to Defendant of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Defendant has a pre-existing legal obligation to employ such measures.

262. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach at Defendant, thus eliminating the additional injuries that would result to Plaintiff and others whose confidential information would be further compromised.

VII. PRAYER FOR RELIEF

WHEREFORE, Plaintiff and the Class pray for judgment against Defendant as follows:

a. An order certifying this action as a class action under R.I. Super. Ct. R. Civ. P. 23, defining the Class as requested herein, appointing the undersigned as Class counsel, and finding that Plaintiff are a proper representative of the Class requested herein;

b. A judgment in favor of Plaintiff and the Class awarding them appropriate monetary relief, including actual and statutory damages, punitive damages,

attorney fees, expenses, costs, and such other and further relief as is just and proper;

c. An order providing injunctive and other equitable relief as necessary to protect the interests of the Class and the general public as requested herein, including, but not limited to:

i. 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 Defendant to promptly correct any problems or issues detected by such third-party security auditors;

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

iii. Ordering that Defendant audit, test, and train its security personnel regarding any new or modified procedures;

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

v. Ordering that Defendant purge, delete, and destroy in a reasonably secure manner customer data not necessary for their provisions of services;

vi. Ordering that Defendant conduct regular database scanning and securing checks; and

vii. 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.

d. An order requiring Defendant to pay the costs involved in notifying the Class members about the judgment and administering the claims process;

e. A judgment in favor of Plaintiff and the Class awarding them pre-judgment and post-judgment interest, reasonable attorneys' fees, costs and expenses as allowable by law; and

f. An award of such other and further relief as this Court may deem just and proper.

VIII. DEMAND FOR JURY TRIAL

Plaintiff demands a trial by jury on all issues so triable.

Dated: January 23, 2025

Respectfully submitted,

/s/ William B. Federman

William B. Federman*
/s/Jessica A. Wilkes
Jessica A. Wilkes*
Federman & Sherwood
10205 N. Pennsylvania Ave
Oklahoma City, OK 73120
(405) 235-1560
wbf@federmanlaw.com
jaw@federmanlaw.com

Counsel for Plaintiff, Bonnie Felingiere and the Proposed Class, Pro Hac Vice Admission Pending

/s/ Christopher E. Hultquist
Christopher E. Hultquist (R.I. Bar # 5264)
Hultquist Law, P.C.
56 Pine Street, Suite 200
Providence, RI 02903
Tel: (401) 383-6650
Fax: (401) 274-2780
hultquistlaw@gmail.com

Local Counsel for Plaintiff Bonnie Felingiere and the Proposed Class