UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS

BEVERLY ROBINSON, *individually and behalf of others similarly situated,* **Plaintiff,** **v.** **BAXTER INTERNATIONAL, INC.** **Defendant.**	**CLASS ACTION** Case No.: **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Plaintiff Beverly Robinson ("Plaintiff"), on behalf of herself and all others similarly situated, alleges the following against Baxter International Inc. ("Baxter" or "Defendant") based upon personal knowledge with respect to herself and on information and belief derived from, among other things, investigation by her counsel and review of public documents, as to all other matters:

NATURE OF THE ACTION

1. Plaintiff brings this class action against Baxter for its failure to properly secure and safeguard Plaintiff's and other similarly situated Baxter customers' and employees' personally identifiable information ("PII") and protected health information ("PHI").

2. Defendant is an American medical equipment manufacturing company that provides medical professionals and patients with healthcare products.[1]

[1] *See* https://www.baxter.com (last visited August 30, 2024).

3. Upon information and belief, former and current customers and employees of Defendant are required to entrust Defendant, directly or indirectly, with sensitive, non-public PII/PHI, without which Defendant could not perform its regular business activities, and employees could not be hired. Defendant retains this information for at least many years and even after the customer relationship has ended.

4. By obtaining, collecting, using, and deriving a benefit from the PII/PHI of Plaintiff and Class Members, Defendant assumed legal and equitable duties to those individuals to protect and safeguard that information from unauthorized access and intrusion.

5. On or about June 10, 2024, Defendant ". . . became aware that an unauthorized third-party downloaded certain files containing personal information from Baxter's network. Baxter took prompt action to respond to this incident, including immediately launching an investigation with the support of outside counsel and leading cybersecurity and forensic experts in order to assess the full impact. The incident has been contained and the investigation has concluded."[2]

6. According to Baxter's report filed with the Office of the California Attorney General, on or about August 8, 2024, the PII/PHI of Baxter's customers and employees was accessed by a unauthorized third party actor on or about June 10, 2024.[3]

7. Defendant failed to adequately protect Plaintiff's and Class Members' PII/PHI—and failed to even encrypt or redact this highly sensitive information. This unencrypted, unredacted PII/PHI was compromised due to Defendant's negligent and/or careless acts and omissions and their utter failure to protect customers' sensitive data. Hackers targeted and obtained Plaintiff's

[2] A sample of the "Notice Letter" is attached hereto as **Exhibit A**.
[3] *See* https://oag.ca.gov/system/files/Baxter%20-%20Template%20Individual%20Letter.pdf

and Class Members' PII/PHI because of its value in exploiting and stealing the identities of Plaintiff and Class Members. The present and continuing risk to victims of the Data Breach will remain for their respective lifetimes.

8. Plaintiff brings this action on behalf of all persons whose PII/PHI was compromised as a result of Defendant's failure to: (i) adequately protect the PII/PHI of Plaintiff and Class Members; (ii) warn Plaintiff and Class Members of Defendant's inadequate information security practices; and (iii) effectively secure hardware containing protected PII/PHI using reasonable and effective security procedures free of vulnerabilities and incidents. Defendant's conduct amounts at least to negligence and violates federal and state statutes.

9. Defendant disregarded the rights of Plaintiff and Class Members by intentionally, willfully, recklessly, or negligently failing to implement and maintain adequate and reasonable measures and ensure those measures were followed 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 PII/PHI of Plaintiff and Class Members was compromised through disclosure to an unknown and unauthorized third party.

10. Plaintiff and Class Members have a continuing interest in ensuring that their information is and remains safe, and they should be entitled to injunctive and other equitable relief.

11. Plaintiff and Class Members have suffered injury as a result of Defendant's conduct. These injuries include: (i) invasion of privacy; (ii) lost or diminished value of PII/PHI; (iii) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (iv) loss of benefit of the bargain; and (v) the continued and certainly increased risk to their PII/PHI, which: (a) remains unencrypted and available for unauthorized third parties

to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII/PHI.

12. Plaintiff and Class Members seek to remedy these harms and prevent any future data compromise on behalf of themselves and all similarly situated persons whose personal data was compromised and stolen as a result of the Data Breach and who remain at risk due to Defendant's inadequate data security practices.

13. Plaintiff seeks remedies including, but not limited to, compensatory damages, nominal damages, and reimbursement of out-of-pocket costs.

14. Plaintiff also seeks injunctive and equitable relief to prevent future injury on behalf of herself and the putative Class.

PARTIES

15. Plaintiff Beverly Robinson, is, and at all times mentioned herein was, an individual citizen of Mississippi and former employee of Defendant. Ms. Robinson learned of the breach after Defendant reported the incident to Office of the California Attorney General, on or about August 8, 2024.[4] Ms. Robinson provided her PII/PHI to Defendant on the condition that it be maintained as confidential and with the understanding that Defendant would employ reasonable safeguards to protect her PII/PHI. If Ms. Robinson had known that Defendant would not adequately protect her PII/PHI, she would not have entrusted Defendant with her PII/PHI or allowed Defendant to maintain or use this sensitive PII/PHI.

16. Defendant Baxter Health Corporation is an Illinois corporation with its principal place of business located in Deerfield, Illinois.

[4] *Id.*

JURISDICTION AND VENUE

17. The Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million, exclusive of interest and costs. The number of class members is over 100, many of whom reside outside the state of Illinois and have different citizenship from Baxter, including Plaintiff. Thus, minimal diversity exists under 28 U.S.C. §1332(d)(2)(A).

18. This Court has jurisdiction over Baxter because Baxter operates in this District.

19. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(a)(1) because Defendant's principal place of business is located in this District, a substantial part of the events giving rise to this action occurred in this District, and Baxter has harmed Class Members residing in this District.

FACTUAL ALLEGATIONS

Defendant's Business

20. Defendant is an American medical equipment manufacturing company that provides medical professionals and patients with healthcare products.[5]

21. Defendant collects PII/PHI from their customers as part of the provision of its services and from their employees as a condition of employment. This PII/PHI includes the PII/PHI which was compromised in the Data Breach alleged herein.

22. Plaintiff Robinson and Class Members are former or current employees and customers of Defendant.

23. In the course of their relationship, Plaintiff and Class Members, provided

[5] *See* https://www.baxter.com (last visited August 30, 2024).

Defendant with personally identifiable information.

24. The information held by Defendant in its computer systems or those of its vendors at the time of the Data Breach included the unencrypted PII/PHI of Plaintiff and Class Members.

25. Upon information and belief, in the course of collecting PII/PHI from customers and employees, including Plaintiff, Defendant promised to provide confidentiality and adequate security for customer data through its applicable privacy policy and through other disclosures in compliance with statutory privacy requirements.

26. Indeed, Defendant's Privacy Policy posted on Defendant's website provides that: " We have reasonable and appropriate security measures in place to protect against the loss, misuse, and alteration of any Personal Information we receive about you."[6]

27. Plaintiff and Class Members, relied on these promises and on this sophisticated business entity to keep their sensitive PII/PHI confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information. Customers and employees, in general, demand security to safeguard their PII/PHI, especially when their Social Security numbers and other sensitive PII/PHI is involved.

28. Plaintiff and the Class Members have taken reasonable steps to maintain the confidentiality of their PII/PHI. Plaintiff and Class Members relied on the sophistication of Defendant to keep their PII/PHI confidential and securely maintained, to use this information for necessary purposes only, and to make only authorized disclosures of this information. Plaintiff and Class Members value the confidentiality of their PII/PHI and demand security to safeguard their PII/PHI.

29. Defendant had a duty to adopt reasonable measures to protect the PII/PHI of

[6] *See* https://www.baxter.com/policies-positions/global-privacy-policy (last visited August 30, 2024)

Plaintiff and Class Members from involuntary disclosure to third parties and to audit, monitor, and verify the integrity of its IT vendors and affiliates. Defendant has a legal duty to keep individuals PII/PHI safe and confidential.

30. Defendant had obligations created by FTC Act, contract, industry standards, and representations made to Plaintiff and Class Members, to keep their PII/PHI confidential and to protect it from unauthorized access and disclosure.

31. Defendant derived a substantial economic benefit from collecting Plaintiff's and Class Members' PII/PHI. Without the required submission of PII/PHI, Defendant could not perform its services or offer employment.

32. 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 disclosure.

The Data Breach

33. On or about August 8, 2024, Defendant, began sending Plaintiff and other Data Breach victims a letter titled Notice of Data Breach (the "Notice"), informing them that:

> **What happened?** On June 10th, 2024, Baxter became aware that an unauthorized third-party downloaded certain files containing personal information from Baxter's network. Baxter took prompt action to respond to this incident, including immediately launching an investigation with the support of outside counsel and leading cybersecurity and forensic experts in order to assess the full impact.
>
> The incident has been contained and the investigation has concluded.
>
> **What are we doing?** We promptly took steps to secure systems and contain the incident. We also deployed additional security measures and tools with the guidance of third-party cybersecurity experts to further strengthen the security of our network.

34. Omitted from the Notice were the details of the root cause of the Data Breach, the

vulnerabilities exploited, and the remedial measures undertaken to ensure such a breach does not occur again. To date, these critical facts have not been explained or clarified to Plaintiff and Class Members, who retain a vested interest in ensuring that their PII/PHI remains protected.

35. This "disclosure" amounts to no real disclosure at all, as it fails to inform, with any degree of specificity, Plaintiff and Class Members of the Data Breach's critical facts. Without these details, Plaintiff's and Class Members' ability to mitigate the harms resulting from the Data Breach is severely diminished.

36. Defendant did not use reasonable security procedures and practices appropriate to the nature of the sensitive information they were maintaining for Plaintiff and Class Members, causing the exposure of PII/PHI, such as encrypting the information or deleting it when it is no longer needed. Moreover, Defendant failed to exercise due diligence in selecting its IT vendors or deciding with whom it would share sensitive PII/PHI.

37. The attacker accessed and acquired files on Defendant's network containing unencrypted PII/PHI of Plaintiff and Class Members. Plaintiff's and Class Members' PII/PHI was accessed and stolen in the Data Breach.

38. Plaintiff further believes her PII/PHI, and that of Class Members, was subsequently sold on the dark web following the Data Breach, as that is the *modus operandi* of cybercriminals that commit cyber-attacks of this type.

39. Due to the actual and imminent risk of identity theft as a result of the Data Breach, Plaintiff and Class Members must, as Defendant's Notice encourages, monitor their financial accounts for many years to mitigate the risk of identity theft.

40. In the Notice Letter posted to the Office of the California Attorney General, Defendant encourages Plaintiff and Class members to place fraud alerts on their credit files is an

acknowledgment that the impacted individuals' PII/PHI was acquired, thereby subjecting Plaintiff and Class Members to a substantial and imminent threat of fraud and identity theft.

41. Defendant had obligations created by the FTC Act, contract, common law, and industry standards to keep Plaintiff's and Class Members' PII/PHI confidential and to protect it from unauthorized access and disclosure.

***Defendant Acquires, Collects, And Stores Employees' and Customers'* PII/PHI**

42. Defendant acquires, collects, shares, and stores a massive amount of PII/PHI on its current and former employees and customers.

43. As a condition of receiving Baxter's services, Defendant requires that current and former employees and customers entrust it with highly sensitive personal information.

44. Defendant retains and stores this information and derives a substantial economic benefit from the PII/PHI that they collect. But for the collection of Plaintiff and Class Members' PII/PHI, Defendant would be unable to offer services or employment to Plaintiff and Class Members.

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

46. Plaintiff and Class Members have taken reasonable steps to maintain the confidentiality of their PII/PHI and would not have entrusted it to Defendant absent a promise to safeguard that information.

47. Plaintiff and Class Members 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.

Data Breaches Are Preventable

48. Defendant could have prevented this Data Breach by, among other things, properly encrypting PII/PHI being shared with its vendors or otherwise ensuring that such PII/PHI was protected while in transit or accessible.

49. Defendant did not use reasonable security procedures and practices appropriate to the nature of the sensitive information they were maintaining for Plaintiff and Class Members, causing the exposure of PII/PHI, such as encrypting the information or deleting it when it is no longer needed.

50. The unencrypted PII/PHI of Class Members will end up for sale to identity thieves on the dark web, if it has not already, or it could 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.

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."[7]

52. To prevent and detect cyber-attacks and/or ransomware attacks Defendant could and should have implemented, as recommended by the United States Government, the following measures:

- Implement an awareness and training program. Because end users are targets, customers 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

[7] 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 August 30, 2024).

(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.[8]

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

53. To prevent and detect cyber-attacks or ransomware attacks 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 privileged credentials;

Thoroughly investigate and remediate alerts

- Prioritize and treat commodity malware infections as potential full compromise;

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].[9]

[9] *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 August 30, 2024).

54. Given that Defendant was storing and sharing the PII/PHI of its current and former employees and customers, Defendant could and should have implemented all of the above measures to prevent and detect cyberattacks.

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

Defendant Knew or Should Have Known of the Risk Because Companies In Possession Of PII/PHI Are Particularly Suspectable To Cyber Attacks

56. Defendant's data security obligations were particularly important given the substantial increase in cyber-attacks and/or data breaches targeting companies that collect and store PII/PHI, like Defendant, preceding the date of the breach.

57. Data thieves regularly target companies like Defendant's due to the highly sensitive information that they custody. Defendant knew and understood that unprotected PII/PHI is valuable and highly sought after by criminal parties who seek to illegally monetize that PII/PHI through unauthorized access.

58. In 2021, a record 1,862 data breaches occurred, resulting in approximately 293,927,708 sensitive records being exposed, a 68% increase from 2020.[10]

59. The 330 reported breaches reported in 2021 exposed nearly 30 million sensitive records (28,045,658), compared to only 306 breaches that exposed nearly 10 million sensitive records (9,700,238) in 2020.[11]

60. Indeed, cyber-attacks, such as the one experienced by Defendant, have become so notorious that the Federal Bureau of Investigation ("FBI") and U.S. Secret Service have issued a

[10] *See* 2021 Data Breach Annual Report (ITRC, Jan. 2022) (available at https://notified.idtheftcenter.org/s/), at 6.
[11] *Id.*

warning to potential targets so they are aware of, and prepared for, a potential attack. As one report explained, smaller entities that store PII are "attractive to ransomware criminals…because they often have lesser IT defenses and a high incentive to regain access to their data quickly."[12]

61. In light of recent high profile data breaches at other industry leading companies, including, Microsoft (250 million records, December 2019), Wattpad (268 million records, June 2020), Facebook (267 million users, April 2020), Estee Lauder (440 million records, January 2020), Whisper (900 million records, March 2020), and Advanced Info Service (8.3 billion records, May 2020), Defendant knew or should have known that the PII/PHI that they collected and maintained would be targeted by cybercriminals.

62. As a custodian of PII/PHI, Defendant knew, or should have known, the importance of safeguarding the PII/PHI entrusted to it by Plaintiff and Class members, and of the foreseeable consequences if its data security systems were breached, including the significant costs imposed on Plaintiff and Class Members as a result of a breach.

63. 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.

64. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the PII/PHI of Plaintiff and Class Members 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.

[12] https://www.law360.com/consumerprotection/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware?nl_pk=3ed44a08-fcc2-4b6c-89f0-aa0155a8bb51&utm_source=newsletter&utm_medium=email&utm_campaign=consumerprotection (last accessed August 30, 2024).

65. Additionally, as companies became more dependent on computer systems to run their business,[13] *e.g.*, working remotely as a result of the Covid-19 pandemic, and the Internet of Things ("IoT"), the danger posed by cybercriminals is magnified, thereby highlighting the need for adequate administrative, physical, and technical safeguards.[14]

66. Defendant was, or should have been, fully aware of the unique type and the significant volume of data on Defendant's server(s), amounting to potentially over one million individuals' detailed, PII/PHI, and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

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

68. 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 bank account and routing numbers—fraudulent use of that information and damage to victims may continue for years.

69. As a company in possession of its current and former employees and customers' PII/PHI, Defendant knew, or should have known, the importance of safeguarding the PII/PHI entrusted to them by Class Members and of the foreseeable consequences if its data security systems were breached. This includes the significant costs imposed on Class Members as a result of a breach. Nevertheless, Defendant failed to take adequate cybersecurity measures to prevent the Data Breach.

[13] https://www.federalreserve.gov/econres/notes/feds-notes/implications-of-cyber-risk-for-financial-stability-20220512.html (last accessed August 30, 2024).
[14] https://www.picussecurity.com/key-threats-and-cyber-risks-facing-financial-services-and-banking-firms-in-2022 (last accessed August 30, 2024).

Value Of Personally Identifiable Information

70. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[15] 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."[16]

71. 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.[17]

72. For example, PII can be sold at a price ranging from $40 to $200.[18] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[19]

73. 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—bank account and routing numbers.

---

[15] 17 C.F.R. § 248.201 (2013).
[16] *Id.*
[17] *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 August 30, 2024).
[18] *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 August 30, 2024).
[19] *In the Dark*, VPNOverview, 2019, *available at*: https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last accessed August 30, 2024).

74. 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 . . . [is] worth more than 10x on the black market."[20]

75. 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.

76. 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.

77. The fraudulent activity resulting from the Data Breach may not come to light for years. There may be a time lag between when harm occurs versus when it is discovered, and also between when PII is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, 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.[21]

78. 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.

---

[20] Tim 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 August 30, 2024).

[21] *Report to Congressional Requesters*, GAO, at 29 (June 2007), *available at:* https://www.gao.gov/assets/gao-07-737.pdf (last accessed August 30, 2024).

Baxter Failed to Comply with FTC Guidelines

79. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision making. Indeed, the FTC has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. *See, e.g., FTC v. Wyndham Worldwide Corp.,* 799 F.3d 236 (3d Cir. 2015).

80. In October 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cybersecurity guidelines for businesses. The guidelines note that businesses should protect the personal customer information that they keep, properly dispose of personal information that is no longer needed, encrypt information stored on computer networks, understand their network's vulnerabilities, and implement policies to correct any security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs, monitor all incoming traffic for activity indicating someone is attempting to hack into the system, watch for large amounts of data being transmitted from the system, and have a response plan ready in the event of a breach.

81. The FTC further recommends that companies not maintain PII/PHI 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 the network for suspicious activity, and verify that third-party service providers have implemented reasonable security measures.

82. The FTC has brought enforcement actions against businesses for failing to

adequately and reasonably protect customer data by 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 the FTCA. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

83. These FTC enforcement actions include actions against insurance companies, like Defendant.

84. As evidenced by the Data Breach, Baxter failed to properly implement basic data security practices and failed to audit, monitor, or ensure the integrity of its vendor's data security practices. Baxter's failure to employ reasonable and appropriate measures to protect against unauthorized access to Plaintiff's and Class Members' PII/PHI constitutes an unfair act or practice prohibited by Section 5 of the FTCA.

85. Baxter was at all times fully aware of its obligation to protect the PII/PHI of its customers yet failed to comply with such obligations. Defendant was also aware of the significant repercussions that would result from its failure to do so.

Baxter Failed to Comply with Industry Standards

86. As noted above, experts studying cybersecurity routinely identify companies like Defendant as being particularly vulnerable to cyberattacks because of the value of the PII/PHI which they collect and maintain.

87. Some industry best practices that should be implemented by companies dealing with sensitive PII/PHI, like Baxter, include but are not limited to: educating all customers, strong password requirements, multilayer security including firewalls, anti-virus and anti-malware software, encryption, multi-factor authentication, backing up data, and limiting which customers can access sensitive data. As evidenced by the Data Breach, Defendant failed to follow some or

all of these industry best practices.

88. Other best cybersecurity practices that are standard include: installing appropriate malware detection software; monitoring and limiting network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches, and routers; monitoring and protecting physical security systems; and training staff regarding these points. As evidenced by the Data Breach, Defendant failed to follow these cybersecurity best practices.

89. 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.

90. Defendant failed to comply with these accepted standards, thereby permitting the Data Breach to occur.

Baxter Breached its Duty to Safeguard Plaintiff's and Class Members' PII/PHI

91. In addition to its obligations under federal and state laws, Baxter owed a duty to Plaintiff and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the PII/PHI in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. Baxter owed a duty to Plaintiff and Class Members to provide reasonable security, including consistency with industry standards and requirements, and to ensure that its computer systems, networks, and protocols adequately protected the PII/PHI of Class Members.

92. Baxter 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 and failed to audit, monitor, or ensure the integrity of its vendor's data security practices. Baxter's unlawful conduct includes, but is not limited to, the following acts and/or omissions:

a. Failing to maintain an adequate data security system that would reduce the risk of data breaches and cyberattacks;

b. Failing to adequately protect current and former customer PII/PHI;

c. Fair to adequately protect current and former employee PII/PHI;

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

e. Failing to audit, monitor, or ensure the integrity of its vendor's data security practices;

f. Failing to sufficiently train its customers and vendors regarding the proper handling of its customers' PII/PHI;

g. Failing to fully comply with FTC guidelines for cybersecurity in violation of the FTCA;

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

i. Otherwise breaching its duties and obligations to protect Plaintiff's and Class Members' PII/PHI.

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

94. Had Baxter remedied the deficiencies in its information storage and security

systems or those of its vendors and affiliates, followed industry guidelines, and adopted security measures recommended by experts in the field, it could have prevented intrusion into its information storage and security systems and, ultimately, the theft of Plaintiff's and Class Members' confidential PII/PHI.

Common Injuries & Damages

95. As a result of Defendant's ineffective and inadequate data security practices, the Data Breach, and the foreseeable consequences of PII/PHI ending up in the possession of criminals, the risk of identity theft to the Plaintiff and Class Members has materialized and is imminent, and Plaintiff and Class Members have all sustained actual injuries and damages, including: (a) invasion of privacy; (b) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft risk; (c) the loss of benefit of the bargain (price premium damages); (d) diminution of value of their PII/PHI; I invasion of privacy; and (f) the continued risk to their PII, which remains in the possession of Defendant, and which is subject to further breaches, so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiff' and Class Members' PII/PHI.

The Data Breach Increases Victims' Risk Of Identity Theft

96. Plaintiff and Class Members are at a heightened risk of identity theft for years to come.

97. The unencrypted PII/PHI of Class Members will end up for sale on the dark web because that is the *modus operandi* of hackers. In addition, unencrypted PII/PHI may 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.

98. 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 below.

99. 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.

100. 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 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.

101. One such example of criminals piecing together bits and pieces of compromised PII for profit is the development of "Fullz" packages.[22]

[22] "Fullz" is fraudster speak for data that includes the information of the victim, including, but not limited to, the name, address, credit card information, social security number, date of birth, and more. As a rule of thumb, the more information you have on a victim, the more money that can be made off of those credentials. Fullz are usually pricier than standard credit card credentials, commanding up to $100 per record (or more) on the dark web. Fullz can be cashed out (turning credentials into money) in various ways, including performing bank transactions over the phone with the required authentication details in-hand. Even "dead Fullz," which are Fullz credentials associated with credit cards that are no longer valid, can still be used for numerous purposes, including tax refund scams, ordering credit cards on behalf of the victim, or opening a "mule account" (an account that will accept a fraudulent money transfer from a compromised account) without the victim's knowledge. *See, e.g.*, Brian Krebs, *Medical Records for Sale in Underground Stolen From Texas Life Insurance Firm*, Krebs on Security (Sep. 18, 2014), https://krebsonsecuritv.eom/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-

102. With "Fullz" packages, 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 of accuracy in order to assemble complete dossiers on individuals.

103. The development of "Fullz" packages means here that the stolen PII/PHI from the Data Breach can easily be used to link and identify it to Plaintiff's and Class Members' 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 that was exfiltrated in the Data Breach, criminals may still 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.

104. 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 driver's license numbers) of Plaintiff and the other Class Members.

105. Thus, even if certain information (such as driver's license numbers) was not stolen in the data breach, criminals can still easily create a comprehensive "Fullz" package.

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

Loss Of Time To Mitigate Risk Of Identity Theft And Fraud

107. As a result of the recognized risk of identity theft, when a Data Breach occurs, and an individual is notified by a company that their PII/PHI was compromised, as in this Data Breach, the reasonable person is expected to take steps and spend time to address the dangerous

insurance-](https://krebsonsecuritv.eom/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-finn/ (last accessed August 30, 2024).

situation, learn about the breach, and otherwise mitigate the risk of becoming a victim of identity theft of fraud. Failure to spend time taking steps to review accounts or credit reports could expose the individual to greater financial harm – yet, the resource and asset of time has been lost.

108. Thus, due to the actual and imminent risk of identity theft, Plaintiff and Class Members must, as Defendant's Notice Letter encourages them, monitor their financial accounts for many years to mitigate the risk of identity theft.

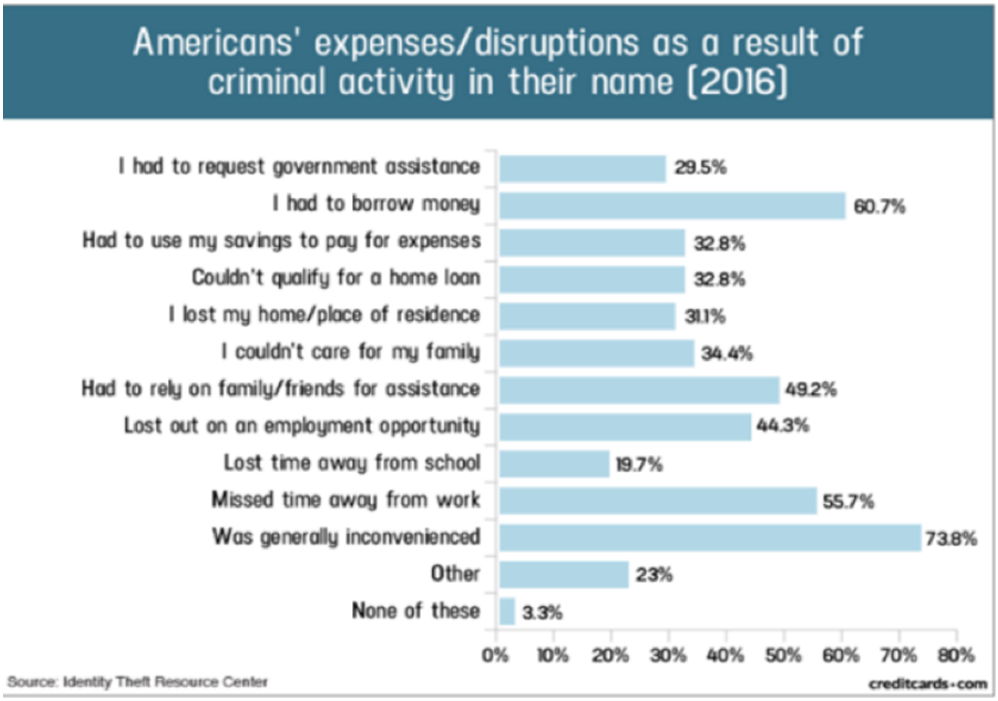
109. Plaintiff and Class Members have spent, and will spend additional time in the future, on a variety of prudent actions to remedy the harms they have or may experience as a result of the Data Breach, such as researching and verifying the legitimacy of the Data Breach upon receiving the Notice Letter.

110. These efforts are consistent with the U.S. Government Accountability Office that released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[23]

111. These efforts are also consistent with the steps that FTC recommends that data breach 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.[24]

[23] *See* United States Government Accountability Office, GAO-07-737, Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown (June 2007), https://www.gao.gov/new.items/d07737.pdf.
[24] *See* Federal Trade Commission, *Identity Theft.gov*, https://www.identitytheft.gov/Steps (last accessed August 30, 2024).

112. A study by Identity Theft Resource Center shows the multitude of harms caused by fraudulent use of personal and financial information:[25]



113. And for those Class Members who experience actual identity theft and fraud, 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 will face "substantial costs and time to repair the damage to their good name and credit record."[26]

Diminution Value Of PII/PHI

114. PII/PHI is a valuable property right.[27] Its value is axiomatic, considering the value

[25] Credit Card and ID Theft Statistics" by Jason Steele, 10/24/2017, at: https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276.php (last accessed August 30, 2024).

[26] *See* "Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown," p. 2, U.S. Government Accountability Office, June 2007, https://www.gao.gov/new.items/d07737.pdf (last accessed August 30, 2024) ("GAO Report").

[27] *See, e.g.,* Randall 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).

of Big Data in corporate America and 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.

115. An active and robust legitimate marketplace for PII/PHI exists. In 2019, the data brokering industry was worth roughly $200 billion.[28]

116. In fact, the data marketplace is so sophisticated that consumers can actually sell their non-public information directly to a data broker who in turn aggregates the information and provides it to marketers or app developers.[29,30]

117. Consumers who agree to provide their web browsing history to the Nielsen Corporation can receive up to $50.00 a year.[31]

118. Conversely sensitive PII can sell for as much as $363 per record on the dark web according to the Infosec Institute.[32]

119. As a result of the Data Breach, Plaintiff's and Class Members' PII/PHI, which has an inherent market value in both legitimate and dark markets, has been damaged and diminished by its compromise and unauthorized release. However, this transfer of value occurred without any consideration paid to Plaintiff or Class Members for their property, resulting in an economic loss. Moreover, the PII/PHI is now readily available, and the rarity of the Data has been lost, thereby causing additional loss of value.

---

[28] https://www.latimes.com/business/story/2019-11-05/column-data-brokers (last accessed August 30, 2024).
[29] https://datacoup.com/ (last accessed August 30, 2024).
[30] https://worlddataexchange.com/about (last accessed August 30, 2024).
[31] Nielsen Computer & Mobile Panel, *Frequently Asked Questions, available at* https://computermobilepanel.nielsen.com/ui/US/en/faqen.html (last accessed August 30, 2024).
[32] *See* Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, InfoSec (July 27, 2015), https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/ (last accessed August 30, 2024).

120. 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.

121. 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.

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

123. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the PII/PHI of Plaintiff and Class Members, 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.

124. Defendant was, or should have been, fully aware of the unique type and the significant volume of data on Defendant's network, amounting to over one million individuals' detailed personal information, upon information and belief, and thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

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

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

126. Given the type of targeted attack in this case and sophisticated criminal activity,

the type of PII/PHI involved, and the volume of data obtained in the Data Breach, 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 for identity theft crimes –*e.g.*, opening bank accounts in the victims' names to make purchases or to launder money; file false tax returns; take out loans or lines of credit; or file false unemployment claims.

127. 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.

128. Consequently, Plaintiff and Class Members are at a present and continuous risk of fraud and identity theft for many years into the future.

129. The retail cost of credit monitoring and identity theft monitoring can cost around $200 a year per Class Member. This is reasonable and necessary cost to monitor 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.

Plaintiff Beverly Robinson's Experience

130. Plaintiff Robinson is a former employee of Baxter.

131. In order to become a prospective employee of Baxter, she was required to provide her PII/PHI to Defendant, including her name, Social Security number, and address.

132. At the time of the Data Breach—approximately June 10, 2024—Defendant retained Plaintiff's PII/PHI in its system.

133. Plaintiff is very careful about sharing her sensitive PII/PHI. Plaintiff stores any documents containing her PII/PHI in a safe and secure location. She has never knowingly transmitted unencrypted sensitive PII/PHI over the internet or any other unsecured source. Plaintiff would not have entrusted her PII/PHI to Defendant had she known of Defendant's lax data security policies.

134. Plaintiff Robinson learned of the breach after receiving a letter from Defendant, on or about August 8, 2024, which told her that her Private Information had been accessed and compromised during the Data Breach.

135. As a result of the Data Breach, and at the direction of Defendant's Notice, Plaintiff made reasonable efforts to mitigate the impact of the Data Breach, including researching and verifying the legitimacy of the Data Breach upon receiving the Notice Letter. Plaintiff has spent significant time dealing with the Data Breach—valuable time Plaintiff otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

136. Plaintiff suffered actual injury from having her PII/PHI compromised as a result of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) lost or diminished value of PII; (iii) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (iv) loss of benefit of the bargain; and (v) the continued and certainly increased risk to their PII/PHI, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII/PHI.

137. The Data Breach has caused Plaintiff to suffer fear, anxiety, and stress, which has

been compounded by the fact that Defendant has still not fully informed her of key details about the Data Breach's occurrence.

138. As a result of the Data Breach, Plaintiff anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

139. As a result of the Data Breach, Plaintiff is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

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

CLASS ACTION ALLEGATIONS

141. Plaintiff brings this action on behalf of herself and as a class action under Fed. R. Civ. P 23(a) and (b), on behalf of the following proposed Class:

> All persons Defendant has identified as being among those individuals impacted by the Data Breach, including all who were sent a notice of the Data Breach (the "Class").

142. Excluded from the Class are Defendant and its parents or subsidiaries, any entities in which it has a controlling interest, as well as its officers, directors, affiliates, legal representatives, heirs, predecessors, successors, and assigns. Also excluded is any Judge to whom this case is assigned as well as their judicial staff and immediate family members.

143. Plaintiff reserves the right to modify or amend the definition of the proposed Classses, as well as add subclasses, before the Court determines whether certification is appropriate.

144. The proposed Class meets the criteria for certification under Fed. R. Civ. P. 23(a), (b)(2), and (b)(3).

145. Numerosity. The Class Members are so numerous that joinder of all members is impracticable. Though the exact number and identities of Class Members are unknown at this time it is likely hundreds, if not thousands of individuals had their PII/PHI compromised in this Data Breach, given the Defendant operates widely throughout the United States. The identities of Class Members are ascertainable through Defendant's records, Class Members' records, publication notice, self-identification, and other means.

146. Commonality. There are questions of law and fact common to the Class which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

a. Whether Baxter engaged in the conduct alleged herein;

b. Whether Baxter's conduct violated the FTCA;

c. When Baxter learned of the Data Breach;

d. Whether Baxter's response to the Data Breach was adequate;

e. Whether Baxter unlawfully lost or disclosed Plaintiff's and Class Members' PII/PHI;

f. Whether Baxter failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the PII/PHI compromised in the Data Breach;

g. Whether Baxter's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

h. Whether Baxter's data security systems prior to and during the Data Breach were consistent with industry standards;

i. Whether Baxter owed a duty to Plaintiff and Class Members to safeguard their

PII/PHI;

j. Whether Baxter breached its duty to Plaintiff and Class Members to safeguard their PII/PHI;

k. Whether hackers obtained Plaintiff's and Class Members' PII/PHI via the Data Breach;

l. Whether Baxter had a legal duty to provide timely and accurate notice of the Data Breach to Plaintiff and the Class Members;

m. Whether Baxter breached its duty to provide timely and accurate notice of the Data Breach to Plaintiff and Class Members;

n. Whether Baxter knew or should have known that its data security systems and monitoring processes were deficient;

o. What damages Plaintiff and Class Members suffered as a result of Baxter's misconduct;

p. Whether Baxter's conduct was negligent;

q. Whether Baxter was unjustly enriched;

r. Whether Plaintiff and Class Members are entitled to actual and/or statutory damages;

s. Whether Plaintiff and Class Members are entitled to additional credit or identity monitoring and monetary relief; and

t. Whether Plaintiff and Class Members are entitled to equitable relief, including injunctive relief, restitution, disgorgement, and/or the establishment of a constructive trust.

147. Typicality. Plaintiff's claims are typical of those of other Class Members because

Plaintiff's PII/PHI, like that of every other Class Member, was compromised in the Data Breach. Plaintiff's claims are typical of those of the other Class Members because, inter alia, all Class Members were injured through the common misconduct of Baxter. Plaintiff is advancing the same claims and legal theories on behalf of herself and all other Class Members, and there are no defenses that are unique to the Plaintiff. The claims of Plaintiff and those of Class Members arise from the same operative facts and are based on the same legal theories.

148. Adequacy of Representation. Plaintiff will fairly and adequately represent and protect the interests of Class Members. Plaintiff's counsel is competent and experienced in litigating class actions, including data privacy litigation of this kind.

149. Predominance. Baxter has engaged in a common course of conduct toward Plaintiff and Class Members in that all of Plaintiff's and Class Members' data was stored on the same computer systems and unlawfully accessed and exfiltrated in the same way. The common issues arising from Baxter's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

150. Superiority. A Class action is superior to other available methods for the fair and efficient adjudication of this controversy and no unusual difficulties are likely to be encountered in the management of this class action. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a Class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Baxter.

In contrast, conducting this action as a class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class Member.

151. Class certification is also appropriate under Fed. R. Civ. P. 23(b)(2). Baxter has acted and/or refused to act on grounds generally applicable to the Class such that final injunctive relief and/or corresponding declaratory relief is appropriate as to the Class as a whole.

152. Finally, all members of the proposed Class are readily ascertainable. Baxter has access to the names and addresses and/or email addresses of Class Members affected by the Data Breach. Class Members have already been preliminarily identified and sent Notice of the Data Breach.

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

153. Plaintiff hereby repeats and realleges paragraphs 1 through 152 of this Complaint and incorporates them by reference herein.

154. Defendant requires its current and former employees and customers, including Class Members, to submit non-public PII/PHI in the ordinary course of providing employment or services.

155. Defendant gathered and stored the PII/PHI of Class Members as part of its business of soliciting its services to its customers, which solicitations and services affect commerce.

156. Defendant gathered and stored the PII/PHI of Plaintiff Robinson and Class Members as part of its practice for offering employment.

157. Plaintiff and Class Members entrusted Defendant with their PII/PHI, directly or indirectly, with the understanding that Defendant would safeguard their information.

158. Defendant had full knowledge of the sensitivity of the PII/PHI and the types of harm that Plaintiff and Class Members could and would suffer if the PII/PHI were wrongfully disclosed.

159. By assuming the responsibility to collect and store this data, and in fact doing so, and sharing it and using it for commercial gain, Defendant had a duty of care to use reasonable means to secure and to prevent disclosure of the information, and to safeguard the information from theft. Defendant's duty included a responsibility to exercise due diligence in selecting IT vendors and to audit, monitor, and ensure the integrity of its vendor's systems and practices and to give prompt notice to those affected in the case of a data breach.

160. Defendant had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

161. Defendant owed a duty of care to Plaintiff and Class Members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that its systems and networks, and the personnel responsible for them, adequately protected the PII/PHI.

162. Defendant's duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendant, Plaintiff and Class Members. That special relationship arose because Plaintiff and the Class entrusted Defendant with their confidential PII/PHI, a necessary part of being customers or employee of Defendant.

163. Defendant's duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendant is

bound by industry standards to protect confidential PII/PHI.

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

165. Defendant also had a duty to exercise appropriate clearinghouse practices to remove current or former employees' and customers' PII/PHI it was no longer required to retain pursuant to regulations.

166. Moreover, Defendant had a duty to promptly and adequately notify Plaintiff and the Class of the Data Breach.

167. Defendant had and continues to have a duty to adequately disclose that the PII/PHI of Plaintiff and the Class within Defendant's possession might have been compromised, how it was compromised, and precisely the types of data that were compromised and when. Such notice was necessary to allow Plaintiff and the Class to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their PII/PHI by third parties.

168. Defendant breached its duties, pursuant to the FTC Act and other applicable standards, and thus was negligent, by failing to use reasonable measures to protect Plaintiff's and Class Members' PII/PHI. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Plaintiff's and Class Members' PII/PHI;

b. Failing to adequately monitor the security of their networks and systems;

c. Failing to audit, monitor, or ensure the integrity of its vendor's data security practices;

d. Allowing unauthorized access to Class Members' PII/PHI;

e. Failing to detect in a timely manner that Plaintiff's and Class Members' PII/PHI had been compromised;

f. Failing to remove current or former employees' and customers' PII/PHI when it was no longer required to retain pursuant to regulations;

g. Failing to timely and adequately notify Plaintiff and Class Members about the Data Breach's occurrence and scope, so that they could take appropriate steps to mitigate the potential for identity theft and other damages; and

h. Failing to secure its stand-alone personal computers, such as the reception desk computers, even after discovery of the data breach.

169. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect 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 the immense damages that would result to Plaintiff and the Class.

170. Plaintiff and Class Members were within the class of persons the Federal Trade Commission Act was intended to protect and the type of harm that resulted from the Data Breach was the type of harm these statues were intended to guard against.

171. Defendant's violation of Section 5 of the FTC Act constitutes negligence.

172. 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.

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

practices.

174. It was foreseeable that Defendant's failure to use reasonable measures to protect Plaintiff's and Class Members' PII/PHI would result in injury to Class Members. Further, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches in the insurance industry.

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

176. Plaintiff and the Class were the foreseeable and probable victims of any inadequate security practices and procedures. Defendant knew or should have known of the inherent risks in collecting and storing the PII/PHI of Plaintiff and the Class, the critical importance of providing adequate security of that PII/PHI, and the necessity for encrypting PII/PHI stored on Defendant's systems.

177. It was therefore foreseeable that the failure to adequately safeguard Plaintiff's and Class Members' PII/PHI would result in one or more types of injuries to Plaintiff and Class Members.

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

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

180. 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 have also recognized the existence of a specific duty to reasonably safeguard personal information.

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

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

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

184. As a direct and proximate result of Defendant's negligence, Plaintiff and the Class have suffered and will suffer injury, including but not limited to: (i) invasion of privacy; (ii) lost or diminished value of PII/PHI; (iii) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (iv) loss of benefit of the bargain; and (v) the continued and certainly increased risk to their PII/PHI, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII/PHI.

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

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

187. Plaintiff and Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

188. Defendant's negligent conduct is ongoing, in that it still holds the PII/PHI of Plaintiff and Class Members in an unsafe and insecure manner.

189. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) continue to provide adequate credit monitoring to all Class Members.

COUNT II
Breach of Implied Contract
(On Behalf Of Plaintiff And the Class)

190. Plaintiff hereby repeats and realleges paragraphs 1 through 152 of this Complaint and incorporate them by reference herein.

191. Plaintiff and Class Members were required to provide their PII/PHI to Defendant as a condition of seeking employment or services from Defendant.

192. Plaintiff and the Class entrusted their PII/PHI to Defendant. In so doing, Plaintiff and the Class entered into implied contracts with Defendant by which Defendant agreed to safeguard and protect such information, to keep such information secure and confidential, and to timely and accurately notify Plaintiff and the Class if their data had been breached and

compromised or stolen.

193. In entering into such implied contracts, Plaintiff and Class Members reasonably believed and expected that Defendant's data security practices complied with relevant laws and regulations and were consistent with industry standards.

194. At the time Defendant acquired the PII/PHI of Plaintiff and the Class, there was a meeting of the minds and a mutual understanding that Defendant would safeguard the PII/PHI and not take unjustified risks when storing the PII/PHI.

195. Implicit in the agreements between Plaintiff and Class Members and Defendant to provide PII/PHI, was the latter's obligation to: (a) use such PII/PHI for business purposes only, (b) take reasonable steps to safeguard that PII/PHI, (c) prevent unauthorized disclosures of the PII/PHI, (d) provide Plaintiff and Class Members with prompt and sufficient notice of any and all unauthorized access and/or theft of their PII/PHI, (e) reasonably safeguard and protect the PII/PHI of Plaintiff and Class Members from unauthorized disclosure or uses, and (f) retain the PII/PHI only under conditions that kept such information secure and confidential.

196. Plaintiff and the Class would not have entrusted their PII/PHI to Defendant had they known that Defendant would make the PII/PHI internet-accessible, not encrypt sensitive data elements such as Social Security numbers, and not delete the PII/PHI that Defendant no longer had a reasonable need to maintain it.

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

198. Defendant breached the implied contracts they made with Plaintiff and the Class by failing to safeguard and protect their personal information, by failing to delete the information of Plaintiff and the Class once the relationship ended, and by failing to provide timely and accurate

notice to them that personal information was compromised because of the Data Breach.

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

200. As a direct and proximate result of Defendant's above-described breach of implied contract, Plaintiff and the Class are entitled to recover actual, consequential, and nominal damages to be determined at trial.

COUNT III
Breach Of Fiduciary Duty
(On Behalf Of Plaintiff And the Class)

201. Plaintiff hereby repeats and realleges paragraphs 1 through 152 of this Complaint and incorporate them by reference herein.

202. In providing their PII/PHI, directly or indirectly, to Defendant, Plaintiff and Class members justifiably placed a special confidence in Defendant to act in good faith and with due regard to interests of Plaintiff and class members to safeguard and keep confidential that PII/PHI.

203. Defendant accepted the special confidence Plaintiff and Class members placed in it, as evidenced by its assertion that it is committed to protecting the privacy of Plaintiff's and Class Members' personal information as detailed in its Privacy Policy.

204. In light of the special relationship between Defendant and Plaintiff and Class members, whereby Defendant became a guardian of Plaintiff's and Class members' PII/PHI, Defendant became a fiduciary by its undertaking and guardianship of the PII/PHI, to act primarily for the benefit of its customers, including Plaintiff and Class members, for the safeguarding of Plaintiff's and Class members' PII/PHI.

205. Defendant has a fiduciary duty to act for the benefit of Plaintiff and Class members upon matters within the scope of its relationship with Defendants' customers and employees, in particular, to keep secure the PII/PHI of its customers and employees.

206. Defendant breached its fiduciary duties to Plaintiff and Class members by failing to protect the integrity of the systems containing Plaintiff's and Class members' PII/PHI.

207. Defendant breached its fiduciary duties to Plaintiff and class members by otherwise failing to safeguard Plaintiff's and Class members' PII/PHI.

208. As a direct and proximate result of Defendant's breaches of its fiduciary duties, Plaintiff and class members have suffered and will suffer injury, including but not limited to: (i) invasion of privacy; (ii) lost or diminished value of PII/PHI; (iii) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (iv) loss of benefit of the bargain; and (v) the continued and certainly increased risk to their PII/PHI, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII/PHI.

209. As a direct and proximate result of Defendant's breaches of its fiduciary duties, Plaintiff and Class members have suffered and will continue to suffer other forms of injury and/or harm, and other economic and non-economic losses.

COUNT IV
Breach Of Confidence
(On Behalf Of Plaintiff And the Class)

210. Plaintiff hereby repeats and realleges paragraphs 1 through 152 of this Complaint and incorporate them by reference herein.

211. At all times during Plaintiff's and Class members' interactions with Defendant, Defendant was fully aware of the confidential, novel, and sensitive nature of Plaintiff's and the Class members' PII/PHI that Plaintiff and Class members provided to Defendant.

212. As alleged herein and above, Defendant's relationship with Plaintiff and Class members was governed by expectations that Plaintiff's and Class members' PII/PHI would be collected, stored, and protected in confidence, and would not be disclosed to unauthorized third parties.

213. Plaintiff and Class members provided their respective PII/PHI to Defendant, directly or indirectly, with the explicit and implicit understandings that Defendant would protect and not permit the PII/PHI to be disseminated to any unauthorized parties.

214. Plaintiff and Class members also provided their respective PII/PHI to Defendant with the explicit understanding that Defendant would take precautions to protect that PII/PHI from unauthorized disclosure, such as following basic principles of information security practices.

215. Defendant voluntarily received in confidence Plaintiff's and Class members' PII/PHI with the understanding that the PII/PHI would not be disclosed or disseminated to the public or any unauthorized third parties.

216. Due to Defendant's failure to prevent, detect, and/or avoid the Data Breach from occurring by, *inter alia*, failing to follow best information security practices to secure Plaintiff's and Class members' PII/PHI, Plaintiff's and Class members' PII/PHI was disclosed and

misappropriated to unauthorized third parties beyond Plaintiff's and Class members' confidence, and without their express permission.

217. But for Defendant's disclosure of Plaintiff's and Class members' PII/PHI in violation of the parties' understanding of confidence, their PII/PHI would not have been compromised, stolen, viewed, accessed, and used by unauthorized third parties. Defendant's Data Breach was the direct and legal cause of the theft of Plaintiff's and Class members' PII/PHI, as well as the resulting damages.

218. The injury and harm Plaintiff and Class members suffered was the reasonably foreseeable result of Defendant's unauthorized disclosure of Plaintiff's and Class members' PII/PHI. Defendant knew or should have known their security systems were insufficient to protect the PII/PHI that is coveted by thieves worldwide. Defendant also failed to observe industry standard information security practices.

219. As a direct and proximate cause of Defendant's conduct, Plaintiff and Class members suffered damages as alleged above.

COUNT V
Invasion of Privacy
(On Behalf Of Plaintiff And the Class)

220. Plaintiff hereby repeats and realleges paragraphs 1 through 152 of this Complaint and incorporate them by reference herein.

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

222. Defendant owed a duty to its current and former customers or employees including Plaintiff and the Class Members, to keep this information confidential.

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

224. The intrusion was into a place or thing which was private and entitled to be private. Plaintiff and Class Members disclosed their sensitive and confidential information to Defendant, but did so privately, with the intention that their information would be kept confidential and protected from unauthorized disclosure. Plaintiff and the Class were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization.

225. The Data Breach constitutes an intentional interference with Plaintiff and the Class Members 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.

226. Defendant acted with a knowing state of mind when it permitted the Data Breach because it knew its information security practices were inadequate.

227. Defendant acted with a knowing state of mind when it failed to notify Plaintiff and Class Members in a timely fashion about the Data Breach, thereby materially impairing their mitigation efforts.

228. Acting with knowledge, Defendant had notice and knew that its inadequate cybersecurity practices would cause injury to Plaintiff and Class Members.

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

230. And, on information and belief, Plaintiff's PII/PHI has already been published—or will be published imminently—by cybercriminals on the Dark Web.

231. Unless and until enjoined and restrained by order of this Court, Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiff and Class Members since their PII/PHI are still maintained by Defendant with their inadequate cybersecurity system and policies.

232. 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 the PII/PHI of Plaintiff and the Class.

233. In addition to injunctive relief, Plaintiff, on behalf of herself and the other Class Members, also 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 VI
Unjust Enrichment / Quasi Contract
(On Behalf Of Plaintiff And the Class)

234. Plaintiff hereby repeats and realleges paragraphs 1 through 152 of this Complaint and incorporate them by reference herein.

235. Plaintiff and Class Members conferred a monetary benefit on Defendant, by providing Defendant with their valuable PII/PHI. In so conferring this benefit, Plaintiff and Class Members understood that part of the benefit Defendant derived from the PII/PHI would be applied to data security efforts to safeguard the PII/PHI.

236. Defendant appreciated that Plaintiff and Class Members were conferring a benefit upon it and accepted that monetary benefit.

237. Acceptance of the benefit under the facts and circumstances described herein make

it inequitable for Defendant to retain that benefit without payment of the value thereof. Specifically, Defendant enriched itself by saving the costs they reasonably should have expended on data security measures to secure Plaintiff's and Class Members' PII/PHI. Instead of providing a reasonable level of security that would have prevented the Data Breach, Defendant instead calculated to avoid their data security obligations at the expense of Plaintiff and Class Members by utilizing cheaper, ineffective security measures. Plaintiff and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's failure to provide the requisite security.

238. Under the principles of equity and good conscience, Defendant should not be permitted to retain the monetary value of the benefit belonging to Plaintiff and Class Members, because Defendant failed to implement appropriate data management and security measures that are mandated by industry standards.

239. Defendant acquired the monetary benefit and PII/PHI through inequitable means in that they failed to disclose the inadequate security practices previously alleged.

240. If Plaintiff and Class Members knew that Defendant had not secured their PII/PHI, they would not have agreed to provide their PII/PHI to Defendant.

241. Plaintiff and Class Members have no adequate remedy at law.

242. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity how their PII/PHI is used; (iii) the compromise, publication, and/or theft of their PII/PHI; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their PII/PHI; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent

researching how to prevent, detect, contest, and recover from identity theft; (vi) the continued risk to their PII/PHI, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect PII/PHI in their continued possession and (vii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII/PHI compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

243. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm.

244. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and Class Members, proceeds that they unjustly received from them.

COUNT X
Declaratory Judgment
(On Behalf of Plaintiff and the Class)

245. Plaintiff hereby repeats and realleges paragraphs 1 through 152 of this Complaint and incorporate them by reference herein.

246. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, *et seq.*, this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and to grant further necessary relief. The Court has broad authority to restrain acts, such as those alleged herein, which are tortious and unlawful.

247. In the fallout of the Data Breach, an actual controversy has arisen about Defendant's various duties to use reasonable data security. On information and belief, Plaintiff alleges that Defendant's actions were—and *still* are—inadequate and unreasonable. And Plaintiff and Class members continue to suffer injury from the ongoing threat of fraud and identity theft.

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

a. Defendant owed—and continues to owe—a legal duty to use reasonable data security to secure the data entrusted to it;

b. Defendant has a duty to notify impacted individuals of the Data Breach under the common law and Section 5 of the FTC Act;

c. Defendant breached, and continues to breach, its duties by failing to use reasonable measures to the data entrusted to it; and

d. Defendant breaches of its duties caused—and continues to cause—injuries to Plaintiff and Class members.

249. The Court should also issue corresponding injunctive relief requiring Defendant to use adequate security consistent with industry standards to protect the data entrusted to it.

250. If an injunction is not issued, Plaintiff and the Class will suffer irreparable injury and lack an adequate legal remedy if Defendant experiences a second data breach.

251. And if a second breach occurs, Plaintiff and the Class will lack an adequate remedy at law because many of the resulting injuries are not readily quantified in full and they will be forced to bring multiple lawsuits to rectify the same conduct. Simply put, monetary damages—while warranted for out-of-pocket damages and other legally quantifiable and provable damages—cannot cover the full extent of Plaintiff's and Class members' injuries.

252. If an injunction is not issued, the resulting hardship to Plaintiff and Class members far exceeds the minimal hardship that Defendant could experience if an injunction is issued.

253. An injunction would benefit the public by preventing another data breach—thus preventing further injuries to Plaintiff, Class members, and the public at large.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff prays for judgment as follows:

A. For an Order certifying this action as a class action and appointing Plaintiff and her counsel to represent the Class;

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

C. For equitable relief compelling Defendant to utilize appropriate methods and policies with respect to consumer data collection, storage, and safety, and to disclose with specificity the type of PII/PHI compromised during the Data Breach;

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

i. Prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;

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

iii. Requiring Defendant to delete, destroy, and purge the PII/PHI of Plaintiff and Class Members unless Defendant can provide to the Court reasonable

justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and Class Members;

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

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

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

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

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

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

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

xi. Requiring Defendant to establish an information security training program that includes at least annual information security training for all patients, with additional training to be provided as appropriate based upon the patients' respective responsibilities with handling personal identifying information, as well as protecting the personal identifying information of Plaintiff and Class Members;

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

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

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

xv. Requiring Defendant to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential

personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves; and

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

xvii. For a period of 10 years, appointing a qualified and independent third party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendant's compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the Class, and to report any deficiencies with compliance of the Court's final judgment.

E. For equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendant's wrongful conduct;

F. Ordering Defendant to pay for not less than ten years of credit monitoring services for Plaintiff and the Class;

G. For an award of actual damages, compensatory damages, statutory damages, and statutory penalties, in an amount to be determined, as allowable by law;

H. For an award of punitive damages, as allowable by law;

I. For an award of attorneys' fees and costs, and any other expense, including expert witness fees;

J. Pre- and post-judgment interest on any amounts awarded; and

K. Such other and further relief as this court may deem just and proper.

JURY TRIAL DEMANDED

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

Dated: September 3, 2024

Respectfully submitted,

SHAMIS & GENTILE P.A.
/s/ Andrew J. Shamis
Andrew J. Shamis, Esq.
Bar No.: 6337427
ashamis@shamisgentile.com
Leanna A. Loginov, Esq.
lloginov@shamisgentile.com
14 NE 1st Ave., Suite 705
Miami, Florida 33132
Telephone: 305-479-2299

Counsel for Plaintiff and the Class