Gary. M. Klinger
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
227 W. Monroe Street, Suite 2100
Chicago, Illinois 60606
Telephone: 866.252.0878
Email: gklinger@milberg.com

James J. Pizzirusso
Hausfeld LLP
888 16th Street, NW, Suite 300
Washington, DC 20006
Phone: (202) 542-7200
Fax: (202) 542-7201
Email: jpizzirusso@hausfeld.com

Attorneys for Plaintiffs and the Proposed Class

Additional Counsel on Signature Page

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
OAKLAND DIVISION

IN RE: POST MEDS, INC. DATA BREACH LITIGATION This Documents Relates To: All Actions	Case No. 4:23-cv-05710-HSG **CONSOLIDATED CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiffs Richard Reed, Frankie Garcia, Michael Siegel, Linda Johnson, David MacDonald, Lasedrick Toles, John Rossi, Michael Thomas, Marissa Porter, Angela Morgan, Benjamin Fisher, Brittany Hallman, Russell Autry, Jacob Benjamin, Victoria Phillips, Christopher Williams, David Sauceda, James Lowery, and Hal Evans ("Plaintiffs"), as individuals and on behalf of all others similarly situated, bring this Class Action Complaint ("Complaint") against

Defendant PostMeds, Inc. d/b/a TruePill ("PostMeds" or "Defendant") and allege, upon personal knowledge as to their own actions and their counsels' investigation, and upon information and belief as to all other matters, as follows:

NATURE OF THE ACTION

1. This class action arises out of the recent cyberattack and data breach ("Data Breach") resulting from PostMeds' failure to implement reasonable and industry standard data security practices.

2. Defendant is a digital pharmacy that "operates a nationwide network of URAC-accredited mail order and specialty pharmacies."[1]

3. Plaintiffs' and Class Members' sensitive personal information—which they entrusted to Defendant on the mutual understanding that Defendant would protect it against disclosure—was compromised and unlawfully accessed due to the Data Breach.

4. As a regular and necessary part of its business PostMeds collected and maintained certain personally identifiable information and protected health information of Plaintiffs and the putative Class Members (defined below), who are (or were) customers at PostMeds.

5. The information compromised in the Data Breach included Plaintiffs' and Class Members' full names, demographic information ("personally identifiable information" or "PII") and medical and health insurance information including, prescription information, medication type, and prescribing physician, which is protected health information ("PHI", and collectively with PII, "Private Information") as defined by the Health Insurance Portability and Accountability Act of 1996 ("HIPAA").

6. The Private Information compromised in the Data Breach was targeted and exfiltrated by cyber-criminals and remains in the hands of those cyber-criminals who target Private Information for its value to identity thieves.

[1] https://www.truepill.com/

7. The Data Breach was a direct result of Defendant's failure to implement adequate and reasonable cyber-security procedures and protocols necessary to protect its patients' Private Information from a foreseeable and preventable cyber-attack.

8. Defendant maintained the Private Information in a reckless manner. In particular, the Private Information was maintained on Defendant's computer network in a condition vulnerable to cyberattacks. Upon information and belief, the mechanism of the cyberattack and potential for improper disclosure of Plaintiffs' and Class Members' Private Information was a known risk to Defendant, and thus, Defendant was on notice that failing to take steps necessary to secure the Private Information from those risks left that property in a dangerous condition.

9. Defendant disregarded the rights of Plaintiffs and Class Members by, *inter alia*, intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure its data systems were protected against unauthorized intrusions; failing to disclose that they did not have adequately robust computer systems and security practices to safeguard Class Members' Private Information; failing to take standard and reasonably available steps to prevent the Data Breach; and failing to provide Plaintiffs and Class Members prompt and accurate notice of the Data Breach.

10. Plaintiffs' and Class Members' identities are now at risk because of Defendant's negligent conduct because the Private Information that Defendant collected and maintained is now in the hands of data thieves.

11. Armed with the Private Information accessed in the Data Breach, data thieves have already engaged in identity theft and fraud and can in the future commit a variety of crimes including, *e.g.*, opening new financial accounts in Class Members' names, taking out loans in Class Members' names, using Class Members' information to obtain government benefits, filing fraudulent tax returns using Class Members' information, obtaining driver's licenses in Class Members' names but with another person's photograph, and giving false information to police during an arrest.

12. As a result of the Data Breach, Plaintiffs and Class Members have been exposed to a heightened and imminent risk of fraud and identity theft. Plaintiffs and Class Members must now and in the future closely monitor their financial accounts to guard against identity theft.

13. Plaintiffs and Class Members may also incur out of pocket costs, *e.g.*, for purchasing credit monitoring services, credit freezes, credit reports, or other protective measures to deter and detect identity theft.

14. Plaintiffs bring this class action lawsuit on behalf all those similarly situated to address Defendant's inadequate safeguarding of Class Members' Private Information that it collected and maintained, and for failing to provide timely and adequate notice to Plaintiffs and other Class Members that their information had been subject to unauthorized access by an unknown third party and precisely what specific type of information was accessed.

15. Through this Complaint, Plaintiffs seek to remedy these harms on behalf of themselves and all similarly situated individuals whose Private Information was accessed during the Data Breach.

PARTIES

16. Plaintiff Richard Reed is a natural person and resident of West Virginia where he intends to remain.

17. Plaintiff David MacDonald is a natural person and resident of California where he intends to remain.

18. Plaintiff Frankie Garcia is a natural person and resident of California where he intends to remain.

19. Plaintiff Jacob Benjamin is a natural person and resident of California where he intends to remain.

20. Plaintiff Christopher Williams is a natural person and resident of California where he intends to remain.

21. Plaintiff Michael Siegel is a natural person and resident of Illinois where he intends to remain.

22. Plaintiff Linda Johnson is a natural person and resident of Mississippi where she intends to remain.

23. Plaintiff John Rossi is a natural person and resident of Florida where he intends to remain.

24. Plaintiff Marissa Porter is a natural person and resident of Florida where she intends to remain.

25. Plaintiff Michael Thomas is a natural person and resident of Texas where he intends to remain.

26. Plaintiff Lasedrick Toles is a natural person and resident of Georgia where he intends to remain.

27. Plaintiff Angela Morgan is a natural person and resident of Tennessee where she intends to remain.

28. Plaintiff Russell Autry is a natural person and resident of Arkansas where he intends to remain.

29. Plaintiff Brittany Hallman is a natural person and resident of South Carolina where she intends to remain.

30. Plaintiff Benjamin Fisher is a natural person and resident of Louisiana where he intends to remain.

31. Plaintiff Victoria Phillips is a natural person and resident of Pennsylvania where she intends to remain.

32. Plaintiff David Sauceda is a natural person and resident of California where he intends to remain.

33. Plaintiff James Lowery is a natural person and resident of Alabama where he intends to remain.

34. Plaintiff Hal Evans is a natural person and resident of New Jersey where he intends to remain.

35. Defendant is a Delaware corporation with its principal place of business located at 3121 Diablo Avenue, Hayward, California 94545.

JURISDICTION AND VENUE

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

37. This Court has personal jurisdiction over Defendant because its principal place of business is in this District, it regularly conducts business in California, and the acts and omissions giving rise to Plaintiffs' claims occurred in and emanated from this District.

38. Venue is proper under 18 U.S.C § 1391(b)(1) because Defendant's principal place of business is in this District.

FACTUAL ALLEGATIONS

Defendant's Business

39. Defendant is a digital pharmacy that "operates a nationwide network of URAC-accredited mail order and specialty pharmacies."[2]

40. Plaintiffs and Class Members are current and former patients of PostMeds.

41. As a condition of obtaining pharmacy services from PostMeds, Plaintiffs and Class Members were required to provide their Private Information to Defendant.

42. The information held by Defendant in its computer systems at the time of the Data Breach included the unencrypted Private Information of Plaintiffs and Class Members.

43. Upon information and belief, in the course of collecting Private Information from its patients, including Plaintiffs, Defendant promised to provide confidentiality and adequate

[2] https://www.truepill.com/

security for customer data through its applicable privacy notice and through other disclosures in compliance with statutory privacy requirements.

44. Indeed, Defendant's Notice of Privacy Practices provides that:

- We are required by law to maintain the privacy and security of your protected health information.
- We will let you know promptly if a breach occurs that may have compromised the privacy or security of your information.
- We must follow the duties and privacy practices described in this notice and give you a copy of it.
- We will not use or share your information other than as described here unless you tell us we can in writing. If you tell us we can, you may change your mind at any time. Let us know in writing if you change your mind.[3]

45. Plaintiffs and Class Members provided their Private Information to Defendant with the reasonable expectation and on the mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access.

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

47. Defendant had a duty to adopt reasonable measures to protect the Private Information of Plaintiffs and Class Members from involuntary disclosure to third parties. Defendant has a legal duty to keep its patients' Private Information safe and confidential.

48. Defendant had obligations created by the FTC Act, HIPAA, contract, industry standards, and representations made to Plaintiffs and Class Members, to keep their Private Information confidential and to protect it from unauthorized access and disclosure.

[3] https://www.truepill.com/legal/nopp

49. Defendant derived a substantial economic benefit from collecting Plaintiffs' and Class Members' Private Information. Without the required submission of Private Information, Defendant could not perform the services it provides.

50. By obtaining, collecting, using, and deriving a benefit from Plaintiffs' and Class Members' Private Information, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiffs' and Class Members' Private Information from disclosure.

The Data Breach

51. On or about October 30, 2023, Defendant began sending Plaintiffs and other Data Breach victims an untitled Notice Letter (the "Notice Letter"), informing them that:

> **What Happened:** On August 31, 2023, we discovered that a bad actor gained access to a subset of files used for pharmacy management and fulfillment services. We immediately launched an investigation with assistance from cybersecurity professionals and worked quickly to secure our environment.
>
> **What Information Was Involved:** Our investigation determined that the bad actor accessed the files between August 30, 2023 and September 1, 2023. One or more of those files contained your name and prescription information. The information varied by individual, but may have included medication type, demographic information, and/or prescribing physician.[4]

52. Omitted from the Notice Letter were any details about what demographic information was compromised, 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 Plaintiffs and Class Members, who retain a vested interest in ensuring that their Private Information remains protected.

53. This "disclosure" amounts to no real disclosure at all, as it fails to inform, with any degree of specificity, Plaintiffs and Class Members of the Data Breach's critical facts.

[4] The "Notice Letter." A sample copy is available at https://assets.website-files.com/650b733c29599811871814e3/65403dd34d99148b02ca8ece_4853-3845-4924-v1.pdf

Without these details, Plaintiffs' and Class Members' ability to mitigate the harms resulting from the Data Breach is severely diminished.

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

55. The attacker accessed and acquired files containing unencrypted Private Information of Plaintiffs and Class Members, including their PHI and other sensitive information. Plaintiffs' and Class Members' Private Information was accessed and stolen in the Data Breach.

56. Certain Plaintiffs have already been informed that their Private Information has been disseminated on the dark web or have suffered from similar misuse of their Private Information, and Plaintiffs believe that the Private Information 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.

Data Breaches Are Preventable

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

58. Defendant could have prevented this Data Breach by, among other things, properly encrypting or otherwise protecting their equipment and computer files containing Private Information.

59. 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:

- Implementing an awareness and training program. Because end users are targets, individuals should be aware of the threat of ransomware and how it is delivered.
- Enabling strong spam filters to prevent phishing emails from reaching the end users and authenticating inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.
- Scanning all incoming and outgoing emails to detect threats and filter executable files from reaching end users.
- Configuring firewalls to block access to known malicious IP addresses.
- Patching operating systems, software, and firmware on devices. Considering using a centralized patch management system.
- Setting anti-virus and anti-malware programs to conduct regular scans automatically.
- Managing 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.
- Configuring 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.
- Disabling macro scripts from office files transmitted via email. Considering using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.
- Implementing 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.
- Considering disabling Remote Desktop protocol (RDP) if it is not being used.
- Using application whitelisting, which only allows systems to execute programs known and permitted by security policy.
- Executing operating system environments or specific programs in a virtualized environment.

- Categorizing data based on organizational value and implementing physical and logical separation of networks and data for different organizational units.[5]

60. 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:

Securing internet-facing assets

- Applying latest security updates
- Using threat and vulnerability management
- Performing regular audit; removing privileged credentials;

Thoroughly investigating and remediating alerts

- Prioritizing and treating commodity malware infections as potential full compromise;

Including IT Pros in security discussions

- Ensuring collaboration among [security operations], [security admins], and [information technology] admins to configure servers and other endpoints securely;

Building credential hygiene

- Using [multifactor authentication] or [network level authentication] and using strong, randomized, just-in-time local admin passwords;

Applying principle of least-privilege

- Monitoring for adversarial activities
- Hunting for brute force attempts
- Monitoring for cleanup of Event Logs
- Analyzing logon events;

Hardening infrastructure

- Using Windows Defender Firewall
- Enabling tamper protection
- Enabling cloud-delivered protection

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

- Turning on attack surface reduction rules and [Antimalware Scan Interface] for Office [Visual Basic for Applications].[6]

61. Given that Defendant was storing the Private Information of its current and former patients, Defendant could and should have implemented all the above measures to prevent and detect cyberattacks.

62. 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, upon information and belief, the exposure of the Private Information of approximately 2.3 million individuals,[7] including that of Plaintiffs and Class Members.

Defendant Acquires, Collects, And Stores Its Customers' Private Information

63. Defendant has historically acquired, collected, stored, and shared the Private Information of Plaintiffs and Class Members.

64. As a condition of obtaining services from PostMeds, Defendant requires that its patients entrust it with highly sensitive personal information.

65. By obtaining, collecting, sharing, and using Plaintiffs' and Class Members' Private Information, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiffs' and Class Members' Private Information from disclosure.

66. Plaintiffs and Class Members have taken reasonable steps to maintain the confidentiality of their Private Information.

67. Defendant could have prevented this Data Breach by properly securing and encrypting the files and file servers containing the Private Information of Plaintiffs and Class Members.

---

[6] *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/

[7] https://www.fiercehealthcare.com/health-tech/digital-pharmacy-startup-truepill-confirms-hackers-accessed-health-data-23m-users

68. Defendant made promises to Plaintiffs and Class Members to maintain and protect their Private Information, demonstrating an understanding of the importance of securing Private Information.

69. Indeed, Defendant's Notice of Privacy Practices provides that:

- We are required by law to maintain the privacy and security of your protected health information.
- We will let you know promptly if a breach occurs that may have compromised the privacy or security of your information.
- We must follow the duties and privacy practices described in this notice and give you a copy of it.
- We will not use or share your information other than as described here unless you tell us we can in writing. If you tell us we can, you may change your mind at any time. Let us know in writing if you change your mind.[8]

70. Plaintiffs and the Class Members relied on Defendant to keep their Private Information confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

Defendant Knew or Should Have Known of the Risk Because Pharmaceutical Companies In Possession Of Private Information Are Particularly Suspectable To Cyber Attacks

71. Defendant's data security obligations were particularly important given the substantial increase in cyber-attacks and/or data breaches targeting healthcare companies that collect and store Private Information, like Defendant, preceding the date of the Data Breach.

72. Data breaches, including those perpetrated against pharmaceutical companies that store Private Information in their systems, have become widespread.

73. In the third quarter of the 2023 fiscal year alone, 7333 organizations experienced data breaches, resulting in 66,658,764 individuals' personal information being compromised.[9]

74. In light of recent high profile cybersecurity incidents at other healthcare partner and provider companies, including HCA Healthcare (11 million patients, July 2023), Managed

[8] https://www.truepill.com/legal/nopp
[9] *See* https://www.idtheftcenter.org/publication/q3-data-breach-2023-analysis/

Care of North America (8 million patients, March 2023), PharMerica Corporation (5 million patients, March 2023), HealthEC LLC (4 million patients, July 2023), ESO Solutions, Inc. (2.7 million patients, September 2023), Prospect Medical Holdings, Inc. (1.3 million patients, July-August 2023), Defendant knew or should have known that its electronic records would be targeted by cybercriminals.

75. 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 warning to potential targets so they are aware of, and prepared for, a potential attack. As one report explained, smaller entities that store Private Information are "attractive to ransomware criminals…because they often have lesser IT defenses and a high incentive to regain access to their data quickly."[10]

76. Defendant knew and understood unprotected or exposed Private Information in the custody of healthcare entities, like Defendant, is valuable and highly sought after by nefarious third parties seeking to illegally monetize that Private Information through unauthorized access.

77. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the Private Information of Plaintiffs 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 Plaintiffs and Class Members as a result of a breach.

78. Plaintiffs 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 Private Information.

[10] 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

79. The injuries to Plaintiffs and Class Members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for the Private Information of Plaintiffs and Class Members.

80. The ramifications of Defendant's failure to keep secure the Private Information of Plaintiffs and Class Members are long lasting and severe. Once Private Information is stolen—particularly PHI—fraudulent use of that information and damage to victims may continue for years.

81. As a healthcare entity in custody of its current and former patients' Private Information, Defendant knew, or should have known, the importance of safeguarding Private Information entrusted to them by Plaintiffs and Class Members, and of the foreseeable consequences if its data security systems were breached. This includes the significant costs imposed on Plaintiffs and Class Members as a result of a breach. Defendant failed, however, to take adequate cybersecurity measures to prevent the Data Breach.

Value Of Personally Identifiable Information

82. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[11]

83. 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."[12]

84. The PII of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web.

85. Numerous sources cite dark web pricing for stolen identity credentials.[13]

[11] 17 C.F.R. § 248.201 (2013).
[12] *Id.*
[13] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends, Oct.

86. For example, PII can be sold at a price ranging from $40 to $200.[14] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[15]

87. PII can sell for as much as $363 per record according to the Infosec Institute.[16] PII is particularly valuable because criminals can use it to target victims with frauds and scams.

88. Identity thieves use stolen PII for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.

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

90. The greater efficiency of electronic health records brings the risk of privacy breaches. These electronic health records contain a lot of sensitive information (*e.g.,* patient data, patient diagnosis, lab results, medications, prescriptions, treatment plans, etc.) that is valuable to cybercriminals. One patient's complete record can be sold for hundreds of dollars on the dark web. As such, PHI/PII is a valuable commodity for which a "cyber black market" exists where criminals openly post stolen payment card numbers, Social Security numbers, and other personal information on several underground internet websites. Unsurprisingly, the pharmaceutical industry is at high risk and is acutely affected by cyberattacks, like the Data Breach here.

91. Between 2005 and 2019, at least 249 million people were affected by healthcare data breaches.[17] Indeed, during 2019 alone, over 41 million healthcare records were exposed,

---

16, 2019, *available at*: https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/

[14] *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/

[15] *In the Dark*, VPNOverview, 2019, *available at*: https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/.

[16] *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/

[17] https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7349636/#B5-healthcare-08-00133/

stolen, or unlawfully disclosed in 505 data breaches.[18] In short, these sorts of data breaches are increasingly common, especially among healthcare systems, which account for 30.03 percent of overall health data breaches, according to cybersecurity firm Tenable.[19]

92. "Medical identity theft is a growing and dangerous crime that leaves its victims with little to no recourse for recovery," reported Pam Dixon, executive director of World Privacy Forum. "Victims often experience financial repercussions and worse yet, they frequently discover erroneous information has been added to their personal medical files due to the thief's activities."[20]

93. A study by Experian found that the average cost of medical identity theft is "about $20,000" per incident and that most victims of medical identity theft were forced to pay out-of-pocket costs for healthcare they did not receive to restore coverage.[21] Almost half of medical identity theft victims lose their healthcare coverage as a result of the incident, while nearly one-third of medical identity theft victims saw their insurance premiums rise, and 40 percent were never able to resolve their identity theft at all.[22]

94. According to account monitoring company LogDog, medical data sells for $50 and up on the dark web.[23]

---

[18] https://www.hipaajournal.com/december-2019-healthcare-data-breach-report/.

[19] https://www.tenable.com/blog/healthcare-security-ransomware-plays-a-prominent-role-incovid-19-era-breaches/

[20] Michael Ollove, "The Rise of Medical Identity Theft in Healthcare," Kaiser Health News, Feb. 7, 2014, https://khn.org/news/rise-of-indentity-theft/

[21] *See* Elinor Mills, "Study: Medical Identity Theft is Costly for Victims," CNET (Mar, 3, 2010), https://www.cnet.com/news/study-medical-identity-theft-is-costly-for-victims/

[22] *Id.; see also Healthcare Data Breach: What to Know About them and What to Do After One,* EXPERIAN, https://www.experian.com/blogs/ask-experian/healthcare-data-breach-what-toknow-about-them-and-what-to-do-after-one/

[23] Lisa Vaas, *Ransomware Attacks Paralyze, and Sometimes Crush, Hospitals*, Naked Security (Oct. 3, 2019), https://nakedsecurity.sophos.com/2019/10/03/ransomware-attacks-paralyze-and-sometimes-crush-hospitals/#content

95. This data, as one would expect, demands a much higher price on the black market than financial data alone. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "[c]ompared to credit card information, personally identifiable information . . . [is] worth more than 10x on the black market."[24]

96. 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.

97. 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 readily 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—names, demographic information, and PHI.

Defendant Fails To Comply With FTC Guidelines

98. 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.

99. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cyber-security guidelines for businesses. These 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.[25]

---

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

[25] *Protecting Personal Information: A Guide for Business*, Federal Trade Commission (2016). Available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf

100. 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 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.[26]

101. The FTC further recommends that companies not maintain Private Information longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

102. The FTC has brought enforcement actions against pharmaceutical companies for failing to protect customer data adequately and reasonably, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential customer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

103. These FTC enforcement actions include actions against healthcare companies, like Defendant.

104. Defendant failed to properly implement basic data security practices.

105. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to patients' Private Information constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

106. Upon information and belief, Defendant was at all times fully aware of its obligation to protect the Private Information of its customers. Defendant was also aware of the significant repercussions that would result from its failure to do so.

[26] *Id.*

Defendant Fails to Comply with HIPAA Guidelines

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

108. Defendant is subject to the rules and regulations for safeguarding electronic forms of medical information pursuant to the Health Information Technology Act ("HITECH").[27] *See* 42 U.S.C. §17921, 45 C.F.R. § 160.103.

109. HIPAA's Privacy Rule or *Standards for Privacy of Individually Identifiable Health Information* establishes national standards for the protection of health information.

110. HIPAA's Privacy Rule or *Security Standards for the Protection of Electronic Protected Health Information* establishes a national set of security standards for protecting health information that is kept or transferred in electronic form.

111. HIPAA requires "compl[iance] with the applicable standards, implementation specifications, and requirements" of HIPAA "with respect to electronic protected health information." 45 C.F.R. § 164.302.

112. "Electronic protected health information" is "individually identifiable health information … that is (i) transmitted by electronic media; maintained in electronic media." 45 C.F.R. § 160.103.

113. HIPAA's Security Rule requires Defendant to do the following:

a. Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits;

[27] HIPAA and HITECH work in tandem to provide guidelines and rules for maintaining protected health information. HITECH references and incorporates HIPAA.

b. Protect against any reasonably anticipated threats or hazards to the security or integrity of such information;

c. Protect against any reasonably anticipated uses or disclosures of such information that are not permitted; and

d. Ensure compliance by its workforce.

114. HIPAA also requires Defendant to "review and modify the security measures implemented … as needed to continue provision of reasonable and appropriate protection of electronic protected health information." 45 C.F.R. § 164.306(e). Additionally, Defendant is required under HIPAA to "[i]mplement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights." 45 C.F.R. § 164.312(a)(1).

115. HIPAA and HITECH also obligated Defendant to implement policies and procedures to prevent, detect, contain, and correct security violations, and to protect against uses or disclosures of electronic protected health information that are reasonably anticipated but not permitted by the privacy rules. *See* 45 C.F.R. § 164.306(a)(1) and § 164.306(a)(3); *see also* 42 U.S.C. §17902.

116. The HIPAA Breach Notification Rule, 45 C.F.R. §§ 164.400-414, also requires Defendant to provide notice of the Data Breach to each affected individual "without unreasonable delay and ***in no case later than 60 days following discovery of the breach***."[28]

117. HIPAA requires a covered entity to have and apply appropriate sanctions against members of its workforce who fail to comply with the privacy policies and procedures of the covered entity or the requirements of 45 C.F.R. Part 164, Subparts D or E. *See* 45 C.F.R. § 164.530(e).

[28] Breach Notification Rule, U.S. Dep't of Health & Human Services, https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html (emphasis added).

118. HIPAA requires a covered entity to mitigate, to the extent practicable, any harmful effect that is known to the covered entity of a use or disclosure of protected health information in violation of its policies and procedures or the requirements of 45 C.F.R. Part 164, Subpart E by the covered entity or its business associate. *See* 45 C.F.R. § 164.530(f).

119. HIPAA also requires the Office of Civil Rights ("OCR"), within the Department of Health and Human Services ("HHS"), to issue annual guidance documents on the provisions in the HIPAA Security Rule. *See* 45 C.F.R. §§ 164.302-164.318. For example, "HHS has developed guidance and tools to assist HIPAA covered entities in identifying and implementing the most cost effective and appropriate administrative, physical, and technical safeguards to protect the confidentiality, integrity, and availability of e-PHI and comply with the risk analysis requirements of the Security Rule." US Department of Health & Human Services, Security Rule Guidance Material.[29] The list of resources includes a link to guidelines set by the National Institute of Standards and Technology (NIST), which OCR says "represent the industry standard for good business practices with respect to standards for securing e-PHI." US Department of Health & Human Services, Guidance on Risk Analysis.[30]

Defendant Fails To Comply With Industry Standards

120. As noted above, experts studying cyber security routinely identify pharmaceutical companies in possession of Private Information as being particularly vulnerable to cyberattacks because of the value of the Private Information which they collect and maintain.

121. Several best practices have been identified that, at a minimum, should be implemented by pharmaceutical companies in possession of Private Information, like Defendant, including but not limited to: educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data and limiting which employees can access

[29] http://www.hhs.gov/hipaa/for-professionals/security/guidance/index.html.
[30] https://www.hhs.gov/hipaa/for-professionals/security/guidance/guidance-risk-analysis/index.html

sensitive data. Defendant failed to follow these industry best practices, including a failure to implement multi-factor authentication.

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

123. 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.

124. These foregoing frameworks are existing and applicable industry standards in the pharmaceutical industry, and upon information and belief, Defendant failed to comply with at least one—or all—of these accepted standards, thereby opening the door to the threat actor and causing the Data Breach.

Defendant's Breach

125. Defendant breached its obligations to Plaintiffs and Class Members and/or was otherwise negligent and reckless by conducting the following acts and/or omissions:

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

b. Failing to adequately protect Private Information;

c. Failing to ensure the confidentiality and integrity of electronic Private Information it created, received, maintained, and/or transmitted;

d. Failing to implement technical policies and procedures for electronic information systems that maintain electronic Private Information to allow access only to those persons or software programs that have been granted access rights;

e. Failing to implement policies and procedures to prevent, detect, contain, and correct security violations;

f. Failing to implement procedures to review records of information system activity regularly, such as audit logs, access reports, and security incident tracking reports;

g. Failing to protect against reasonably anticipated threats or hazards to the security or integrity of electronic Private Information;

h. Failing to train all members of their workforce effectively on the policies and procedures regarding Private Information;

i. Failing to render the electronic Private Information it maintained unusable, unreadable, or indecipherable to unauthorized individuals;

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

k. Failing to adhere to HIPAA guidelines and industry standards for cybersecurity as discussed above; and,

l. Otherwise breaching their duties and obligations to protect Plaintiff's and Class Members' Private Information.

126. Defendant negligently and unlawfully failed to safeguard Plaintiffs' and Class Members' Private Information by allowing cyberthieves to access Defendant's online insurance application flow, which provided unauthorized actors with unsecured and unencrypted Private Information.

127. Had Defendant remedied the deficiencies in its information storage and security systems, 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 Plaintiffs' and Class Members' confidential Private Information.

128. Accordingly, as outlined below, Plaintiffs and Class Members now face a present, increased risk of fraud and identity theft. In addition, Plaintiffs and the Class Members lost the benefit of the bargain they made with Defendant.

COMMON INJURIES & DAMAGES

129. As a result of Defendant's ineffective and inadequate data security practices, the Data Breach, and the foreseeable consequences of Private Information ending up in the possession of criminals, the risk of identity theft to the Plaintiffs and Class Members has materialized and is imminent, and Plaintiffs and Class Members have all sustained actual injuries and damages, including: (i) invasion of privacy; (ii) theft of their Private Information; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) statutory damages; (viii) nominal damages; and (ix) the continued and certainly increased risk to their Private Information, 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 Private Information.

The Data Breach Increases Victims' Risk Of Identity Theft

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

131. As Plaintiffs have already experienced, the unencrypted Private Information of Class Members will end up for sale on the dark web because that is the *modus operandi* of hackers. In addition, unencrypted Private Information may fall into the hands of companies that will use the detailed Private Information for targeted marketing without the approval of Plaintiffs and Class Members. Unauthorized individuals can easily access the Private Information of Plaintiffs and Class Members.

132. The link between a data breach and the risk of identity theft is simple and well established. Criminals acquire and steal Private Information 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.

133. 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.

134. 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.

135. One such example of criminals piecing together bits and pieces of compromised Private Information for profit is the development of "Fullz" packages.[31]

[31] "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-

136. With "Fullz" packages, cyber-criminals can cross-reference two sources of Private Information to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy to assemble complete dossiers on individuals.

137. The development of "Fullz" packages means here that the stolen Private Information from the Data Breach can easily be used to link and identify it to Plaintiffs' 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 Private Information 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.

138. The existence and prevalence of "Fullz" packages means that the Private Information stolen from the Data Breach can easily be linked to the unregulated data (like phone numbers and emails) of Plaintiffs and the other Class Members.

139. Thus, even if certain information (such as Social Security numbers) was not stolen in the Data Breach, criminals can still easily create a comprehensive "Fullz" package.

140. 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

141. 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 Private Information was compromised, as in this Data Breach, the reasonable person is expected to take steps and spend time to address the dangerous 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

---

texas-life-insurance-](https://krebsonsecuritv.eom/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-finn/

could expose the individual to greater financial harm – yet, the resource and asset of time has been lost.

142. Thus, due to the actual and imminent risk of identity theft, Defendant's Notice Letter encourages Plaintiffs and Class Members to do the following: "We also encourage you to regularly review your information for accuracy, as a best practice, including information you receive from your healthcare providers."[32]

143. Due to the actual and imminent risk of identity theft, Plaintiffs and Class Members must, as Defendant's Notice Letter encourages, monitor their financial accounts for many years to mitigate the risk of identity theft.

144. Plaintiffs and Class Members have spent, and will spend additional time in the future, on a variety of prudent actions, such as researching and verifying the legitimacy of the Data Breach upon receiving the Notice Letter, changing passwords and resecuring their own computer networks; and contacting companies regarding suspicious activity on their accounts.

145. Plaintiffs' mitigation 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."[33]

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

---

[32] Notice Letter.

[33] *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.

[34] *See* Federal Trade Commission, *Identity Theft.gov*, https://www.identitytheft.gov/Steps.

Diminution Value Of Private Information

147. PII and PHI are valuable property rights.[35] Their value is axiomatic, considering the value 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 Private Information has considerable market value.

148. An active and robust legitimate marketplace for PII exists. In 2019, the data brokering industry was worth roughly $200 billion.[36]

149. 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.[37,38]

150. Consumers who agree to provide their web browsing history to the Nielsen Corporation can receive up to $50.00 a year.[39]

151. Conversely sensitive PII can sell for as much as $363 per record on the dark web according to the Infosec Institute.[40]

152. According to account monitoring company LogDog, medical data sells for $50 and up on the dark web.[41]

153. As a result of the Data Breach, Plaintiffs' and Class Members' Private Information, which has an inherent market value in both legitimate and dark markets, has been

---

[35] *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).

[36] https://www.latimes.com/business/story/2019-11-05/column-data-brokers

[37] https://datacoup.com/

[38] https://digi.me/what-is-digime/

[39] Nielsen Computer & Mobile Panel, Frequently Asked Questions, available at https://computermobilepanel.nielsen.com/ui/US/en/faqen.html

[40] *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/

[41] Lisa Vaas, *Ransomware Attacks Paralyze, and Sometimes Crush, Hospitals*, Naked Security (Oct. 3, 2019), https://nakedsecurity.sophos.com/2019/10/03/ransomware-attacks-paralyze-and-sometimes-crush-hospitals/#content

damaged and diminished by its compromise and unauthorized release. However, this transfer of value occurred without any consideration paid to Plaintiffs or Class Members for their property, resulting in an economic loss. Moreover, the Private Information is now readily available, and the rarity of the data has been lost, thereby causing additional loss of value.

154. 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.

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

156. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the Private Information of Plaintiffs 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 Plaintiffs and Class Members as a result of a Data Breach.

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

158. The injuries to Plaintiffs and Class Members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for the Private Information of Plaintiffs and Class Members.

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

159. Given the type of targeted attack in this case and sophisticated criminal activity, the type of Private Information involved, the volume of data obtained in the Data Breach, and Plaintiffs' Private Information already being disseminated on the dark web (as discussed below), 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 Private Information 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.

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

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

162. The retail cost of credit monitoring and identity theft monitoring can cost around $200 a year per Class Member. This is a reasonable and necessary cost to monitor to protect Class Members from the risk of identity theft that arose from Defendant's Data Breach.

Loss Of The Benefit Of The Bargain

163. Furthermore, Defendant's poor data security deprived Plaintiffs and Class Members of the benefit of their bargain. When agreeing to obtain services from Defendant under certain terms, Plaintiffs and other reasonable customers understood and expected that they were, in part, paying for services and data security to protect their Private Information, when in fact, Defendant did not provide the expected data security. Accordingly, Plaintiffs and Class Members received services that were of a lesser value than what they reasonably expected to receive under the bargains they struck with Defendant.

PLAINTIFFS' EXPERIENCES

Plaintiff Reed

164. Plaintiff Richard Reed is a current PostMeds customer.

165. As a condition of obtaining services at PostMeds, Plaintiff Reed was required to provide his Private Information to Defendant, including his name, demographic information, and PHI.

166. At the time of the Data Breach—August 30, 2023 through September 1, 2023—Defendant retained Plaintiff Reed's Private Information in its system.

167. Plaintiff Reed is very careful about sharing his sensitive Private Information. Plaintiff stores any documents containing his Private Information in a safe and secure location. He has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source. Plaintiff Reed would not have entrusted his Private Information to Defendant had he known of Defendant's lax data security policies.

168. Plaintiff Reed received the Notice Letter, by U.S. mail, directly from Defendant, dated October 30, 2023. According to the Notice Letter, Plaintiff's Private Information was improperly accessed and obtained by unauthorized third parties, including his name, prescription information, medication type, demographic information, and/or prescribing physician.

169. As a result of the Data Breach, and at the direction of Defendant's Notice Letter, Plaintiff Reed 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, changing passwords and resecuring his own computer network, and contacting companies regarding suspicious activity on his accounts. Plaintiff Reed 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.

170. Plaintiff Reed further suffered actual injury in the form of his Private Information being disseminated on the dark web, according to CreditWise and Experian, which, upon information and belief, was caused by the Data Breach.

171. Plaintiff Reed further suffered actual injury in the form of his credit score being damaged, which, upon information and belief, was caused by the Data Breach.

172. Plaintiff Reed further suffered actual injury in the form of experiencing suspicious activity on his Venmo account, including certain account information being changed, which, upon information and belief, was caused by the Data Breach.

173. Plaintiff Reed further suffered actual injury in the form of experiencing an increase in spam calls, texts, and/or emails, which, upon information and belief, was caused by the Data Breach.

174. The Data Breach has caused Plaintiff Reed to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendant has still not fully informed him of key details about the Data Breach's occurrence.

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

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

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

Plaintiff McDonald

178. Defendant obtained Plaintiff McDonald's sensitive Private Information pursuant to Plaintiff's use of the pharmacy company RxLocal—a company that uses Defendant's pharmacy-related products and/or services. Plaintiff McDonald discovered this upon calling the hotline number provided by Defendant.

179. Thus, Defendant obtained and maintained Plaintiff McDonald's Private Information at the time of the Data Breach.

180. When Plaintiff McDonald provided his Private Information to Defendant, he trusted that Defendant would use reasonable measures to protect it according to Defendant's internal policies, as well as state and federal law. Defendant obtained and continues to maintain Plaintiff McDonald's Private Information and has a continuing legal duty and obligation to protect that Private Information from unauthorized access and disclosure.

181. Plaintiff McDonald received a Notice Letter on November 6, 2023 informing him that through its Data Breach, Defendant compromised Plaintiff's name and medical information.

182. Plaintiff McDonald has spent—and will continue to spend—significant time and effort monitoring his accounts to protect himself from identity theft. After all, Defendant directed Plaintiff to take those steps in its Notice Letter.

183. And in the aftermath and as a result of the Data Breach, Plaintiff McDonald has suffered from a spike in spam messages and phone calls that he believes are attempts to acquire further personal information from him.

184. The Data Breach has caused Plaintiff McDonald to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendant has still not fully informed him of key details about the Data Breach's occurrence.

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

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

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

Plaintiff Garcia

188. As a condition of obtaining services from PostMeds, Plaintiff Garcia was required to provide his Private Information to Defendant, including his name, demographic information, and PHI.

189. Plaintiff Garcia's PII, including his name, prescription information, mediation types, demographic information, and/or prescribing physician, among other personal, sensitive and confidential information, were in the possession, custody and/or control of PostMeds at the time of the Data Breach. Plaintiff believed that PostMeds would protect and keep his PII

protected, secure and safe from unlawful disclosure. Plaintiff Garcia would not have entrusted his PII to Defendant had he known of Defendant's lax data security policies.

190. After the Data Breach, Plaintiff Garcia received a Notice Letter from PostMeds via letter dated October 30, 2023.

191. At the direction of Defendant's Notice Letter, Plaintiff Garcia has spent and will continue to spend time and effort monitoring his accounts to protect himself from identity theft. Plaintiff remains concerned for his personal security and the uncertainty of what personal information was exposed to hackers and/or posted to the dark web.

192. As a direct and foreseeable result of PostMeds' failure to implement and maintain reasonable data security Plaintiff Garcia continues to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendant has still not fully informed him of key details about the Data Breach's occurrence.

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

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

Plaintiff Benjamin

195. As a condition to obtaining services at PostMeds, Plaintiff Benjamin was required to provide his Private Information to Defendant.

196. On October 30, 2023, Plaintiff Benjamin received a Notice Letter, which stated that Plaintiff Benjamin's name and prescription information were compromised in the Data Breach.

197. The confidentiality of Plaintiff Benjamin's sensitive information has been irreparably harmed. For the rest of his life, Plaintiff Benjamin will have to worry about when and how his sensitive information may be shared or used to his detriment.

198. As a result of the Data Breach, Plaintiff Benjamin spent time dealing with the consequences of the Data Breach, which includes time spent verifying the legitimacy of the Notice Letter and self-monitoring his accounts.

199. Plaintiff Benjamin is very careful about not sharing his sensitive Private Information. He has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source.

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

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

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

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

Plaintiff Williams

204. As a condition to obtaining services at PostMeds, Plaintiff Williams was required to provide his Private Information to Defendant.

205. On or about October 31, 2023, PostMeds notified Plaintiff Williams that his highly sensitive and confidential Private Information was compromised as a result of unauthorized access to PostMeds files.

206. Plaintiff Williams would not have provided his Private Information to Defendant or any affiliates of Defendant if Plaintiff had known that Defendant's data security measures were inadequate to protect his data.

207. As a result of the Data Breach, and at the direction of Defendant's Notice Letter, Plaintiff Willaims made reasonable efforts to mitigate the impact of the Data Breach, including researching and verifying the legitimacy of the Data Breach upon receiving notice and reviewing his accounts. Plaintiff Williams has spent significant time dealing with this Data Breach.

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

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

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

Plaintiff Siegel

211. Plaintiff Siegel obtained pharmacy or related healthcare services from PostMeds. As a condition of receiving such services, PostMeds required Plaintiff to provide it with his Private Information.

212. Based on representations made by PostMeds, Plaintiff Siegel believed that PostMeds had implemented and maintained reasonable security and practices to protect his Private Information. With this belief in mind, Plaintiff provided his Private Information to PostMeds in connection with receiving pharmacy or related services provided by PostMeds.

213. At the time of the Data Breach, PostMeds stored and maintained Plaintiff Siegel's Private Information on its network systems.

214. Plaintiff Siegel takes great care to protect his Private Information. Had he known that PostMeds does not adequately protect the Private Information in its possession, he would not have obtained pharmacy services from PostMeds or agreed to entrust it with his Private Information.

215. Plaintiff received a Notice Letter from PostMeds notifying him that his Private Information was compromised in the Data Breach.

216. As a direct result of the Data Breach, Plaintiff Siegel has suffered injury and damages including, *inter alia*, a substantial and imminent risk of identity theft and medical identity theft; the wrongful disclosure and loss of confidentiality of his highly sensitive Private Information; deprivation of the value of his Private Information; and overpayment for services that did not include adequate data security.

217. As a result of the Data Breach, and at the direction of Defendant's Notice Letter, Plaintiff Siegel made reasonable efforts to mitigate the impact of the Data Breach. Plaintiff Siegel has spent significant time dealing with this Data Breach.

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

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

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

Plaintiff Johnson

221. Plaintiff Johnson provided her Private Information to her PostMeds, either directly or indirectly, in connection with her obtaining pharmacy services from Defendant. Plaintiff trusted that this information would be safeguarded according to state and federal law.

222. Upon information and belief, Defendant received and maintains the information Plaintiff Johnson was required to provide to her doctors or medical professionals in connection with obtaining pharmacy services from Defendant.

223. Plaintiff Johnson is very careful with her Private Information. She stores any documents containing her Private Information in a safe and secure location or destroys the

documents. Plaintiff has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source. Moreover, Plaintiff diligently chooses unique usernames and passwords for her various online accounts.

224. As a result of the Data Breach, Plaintiff Johnson made reasonable efforts to mitigate the impact of the Data Breach after receiving the Notice Letter, including but not limited to researching the Data Breach, reviewing credit card and financial account statements, and monitoring her credit.

225. Plaintiff Johnson was forced to spend multiple hours attempting to mitigate the effects of the Data Breach. She will continue to spend valuable time she otherwise would have spent on other activities, including but not limited to work and/or recreation. This is time that is lost forever and cannot be recaptured.

226. Plaintiff Johnson has also suffered emotional distress that is proportional to the risk of harm and loss of privacy caused by the theft of her Private Information, which she believed would be protected from unauthorized access and disclosure, including anxiety about unauthorized parties viewing, selling, and/or using her Private Information for purposes of identity theft and fraud. Plaintiff has also suffered anxiety about unauthorized parties viewing, using, and/or publishing information related to her private health conditions and medication prescriptions.

227. As a result of the Data Breach, Plaintiff Johnson anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. In addition, Plaintiff will continue to be at present, imminent, and continued increased risk of identity theft and fraud in perpetuity.

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

Plaintiff Rossi

229. In order to receive pharmaceutical services, Defendant required Plaintiff Rossi provide it with substantial amounts of his Private Information.

230. On or about October 30, 2023, Plaintiff Rossi received a letter which told him that his Private Information had been accessed during the Data Breach. The Notice Letter informed him that the information stolen included his "name and prescription information."

231. The Notice Letter declined to offer Plaintiff Rossi any complimentary credit monitoring services. Failing to offer credit monitoring is unacceptable given that Plaintiff Rossi will now experience a lifetime of increased risk of identity theft, including but not limited to, potential medical fraud.

232. Plaintiff Rossi suffered actual injury in the form of time spent dealing with the Data Breach and the increased risk of fraud resulting from the Data Breach and/or monitoring his accounts for fraud.

233. Plaintiff Rossi would not have provided his Private Information to Defendant had Defendant timely disclosed that its systems lacked adequate computer and data security practices to safeguard its patients' personal and health information from theft, and that those systems were subject to a data breach.

234. Plaintiff Rossi suffered actual injury in the form of having his Private Information compromised and/or stolen as a result of the Data Breach.

235. Plaintiff Rossi suffered actual injury in the form of damages to and diminution in the value of his personal, health, and financial information – a form of intangible property that Plaintiff Rossi entrusted to Defendant for the purpose of receiving healthcare services from Defendant and which was compromised in, and as a result of, the Data Breach.

236. Plaintiff Rossi suffered imminent and impending injury arising from the substantially increased risk of future fraud, identity theft, and misuse posed by his Private Information being placed in the hands of criminals.

237. Plaintiff Rossi has a continuing interest in ensuring that his Private Information, which remain in the possession of Defendant, is protected and safeguarded from future breaches.

238. As a result of the Data Breach, Plaintiff Rossi made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to researching the Data Breach, reviewing financial accounts for any indications of actual or attempted identity theft or fraud, and researching the credit monitoring offered by Defendant. Plaintiff Rossi has spent several hours dealing with the Data Breach, valuable time he otherwise would have spent on other activities.

239. As a result of the Data Breach, Plaintiff Rossi has suffered anxiety as a result of the release of his Private Information, which he believed would be protected from unauthorized access and disclosure. These feelings include anxiety about unauthorized parties viewing, selling, and/or using his Private Information for purposes of committing cyber and other crimes against him including, but not limited to, medical fraud, and identity theft. Plaintiff Rossi is very concerned about this increased, substantial, and continuing risk, as well as the consequences that identity theft and fraud resulting from the Data Breach would have on his life.

240. Plaintiff Rossi also suffered actual injury from having his Private Information compromised as a result of the Data Breach in the form of (a) damage to and diminution in the value of his Private Information, a form of property that Defendant obtained from Plaintiff Rossi; (b) violation of his privacy rights; and (c) present, imminent, and impending injury arising from the increased risk of identity theft, and fraud he now faces.

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

Plaintiff Porter

242. In order to receive pharmaceutical services, Defendant required Plaintiff Porter provide it with substantial amounts of her Private Information.

243. On or about October 30, 2023, Plaintiff Porter received a letter which told her that her Private Information I had been accessed during the Data Breach. The Notice Letter informed her that the information stolen included her "name and prescription information."

244. The Notice Letter declined to offer Plaintiff Porter any complimentary credit monitoring services. Failing to offer credit monitoring is unacceptable given that Plaintiff Porter will now experience a lifetime of increased risk of identity theft, including but not limited to, potential medical fraud.

245. Soon after the Data Breach, Plaintiff Porter suffered actual injury in the form of a substantial decrease in her credit score beginning on September 1, 2023, as well as the suspicious and unauthorized closure of two of her financial card accounts. In addition, she also suffered actual injury in the form of lost time spent dealing with the Data Breach and the increased risk of additional fraud, including medical fraud, resulting from the Data Breach, and monitoring her accounts for fraud.

246. Plaintiff Porter would not have provided her Private Information to Defendant had Defendant timely disclosed that its systems lacked adequate computer and data security practices to safeguard its patients' personal and health information from theft, and that those systems were subject to a data breach.

247. Plaintiff Porter suffered actual injury in the form of having her Private Information compromised and/or stolen as a result of the Data Breach.

248. Plaintiff Porter suffered actual injury in the form of damages to and diminution in the value of her personal, health, and financial information – a form of intangible property that Plaintiff Porter entrusted to Defendant for the purpose of receiving healthcare services from Defendant and which was compromised in, and as a result of, the Data Breach.

249. Plaintiff Porter suffered imminent and impending injury arising from the substantially increased risk of future fraud, identity theft, and misuse posed by her Private Information being placed in the hands of criminals.

250. Plaintiff Porter has a continuing interest in ensuring that her Private Information, which remain in the possession of Defendant, are protected and safeguarded from future breaches.

251. As a result of the Data Breach, Plaintiff Porter made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to researching the Data Breach, reviewing financial accounts for any indications of actual or attempted identity theft or fraud, and researching the credit monitoring offered by Defendant. Plaintiff Porter has spent several hours dealing with the Data Breach, valuable times she otherwise would have spent on other activities.

252. As a result of the Data Breach, Plaintiff Porter has suffered anxiety as a result of the release of her Private Information, which she believed would be protected from unauthorized access and disclosure. These feelings include anxiety about unauthorized parties viewing, selling, and/or using her Private Information for purposes of committing cyber and other crimes against her including, but not limited to, medical fraud, and identity theft. Plaintiff Porter is very concerned about this increased, substantial, and continuing risk, as well as the consequences that identity theft and fraud resulting from the Data Breach would have on her life.

253. Plaintiff Porter also suffered actual injury from having her Private Information compromised as a result of the Data Breach in the form of (a) damage to and diminution in the value of her Private Information, a form of property that Defendant obtained from Plaintiff Porter; (b) violation of her privacy rights; and (c) present, imminent, and impending injury arising from the increased risk of identity theft, and fraud she now faces.

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

Plaintiff Thomas

255. In order to receive pharmaceutical services, Defendant required Plaintiff Thomas to provide it with substantial amounts of his Private Information.

256. On or about October 30, 2023, Plaintiff Thomas received a letter which told him that his Private Information had been accessed during the Data Breach. The Notice Letter informed him that the information stolen included his "name and prescription information."

257. The Notice Letter declined to offer Plaintiff Thomas any complimentary credit monitoring services. Failing to offer credit monitoring is unacceptable given that Plaintiff Thomas will now experience a lifetime of increased risk of identity theft, including but not limited to, potential medical fraud.

258. Plaintiff Thomas suffered actual injury in the form of time spent dealing with the Data Breach and the increased risk of fraud resulting from the Data Breach and/or monitoring his accounts for fraud.

259. Plaintiff Thomas would not have provided his Private Information to Defendant had Defendant timely disclosed that its systems lacked adequate computer and data security practices to safeguard its patients' personal and health information from theft, and that those systems were subject to a data breach.

260. Plaintiff Thomas suffered actual injury in the form of having his Private Information compromised and/or stolen as a result of the Data Breach.

261. Plaintiff Thomas suffered actual injury in the form of damages to and diminution in the value of his personal, health, and financial information – a form of intangible property that Plaintiff Thomas entrusted to Defendant for the purpose of receiving healthcare services from Defendant and which was compromised in, and as a result of, the Data Breach.

262. Plaintiff Thomas suffered imminent and impending injury arising from the substantially increased risk of future fraud, identity theft, and misuse posed by his Private Information being placed in the hands of criminals.

263. Plaintiff Thomas has a continuing interest in ensuring that his Private Information, which remain in the possession of Defendant, is protected and safeguarded from future breaches.

264. As a result of the Data Breach, Plaintiff Thomas made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to researching the Data Breach,

reviewing financial accounts for any indications of actual or attempted identity theft or fraud, and researching the credit monitoring offered by Defendant. Plaintiff Thomas has spent several hours dealing with the Data Breach, valuable time he otherwise would have spent on other activities.

265. As a result of the Data Breach, Plaintiff Thomas has suffered anxiety as a result of the release of his Private Information, which he believed would be protected from unauthorized access and disclosure. These feelings include anxiety about unauthorized parties viewing, selling, and/or using his Private Information for purposes of committing cyber and other crimes against him including, but not limited to, medical fraud, and identity theft. Plaintiff Thomas is very concerned about this increased, substantial, and continuing risk, as well as the consequences that identity theft and fraud resulting from the Data Breach would have on his life.

266. Plaintiff Thomas also suffered actual injury from having his Private Information compromised as a result of the Data Breach in the form of (a) damage to and diminution in the value of his Private Information, a form of property that Defendant obtained from Plaintiff Thomas; (b) violation of his privacy rights; and (c) present, imminent, and impending injury arising from the increased risk of identity theft, and fraud he now faces.

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

Plaintiff Toles

268. Defendant received highly sensitive Private Information from Plaintiff Toles in connection with the services provided by PostMeds. As a result, Plaintiff Toles' information was among the data an unauthorized third party accessed in the Data Breach.

269. Plaintiff Toles is very careful about sharing his Private Information. Plaintiff has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source.

270. Plaintiff Toles stores any documents containing his Private Information in a safe and secure location or destroys the documents. Moreover, Plaintiff Toles diligently chose unique usernames and passwords for his various online accounts.

271. Plaintiff Toles took reasonable steps to maintain the confidentiality of his Private Information and relied on Defendant to keep his Private Information confidential and securely maintained, to use this information for healthcare purposes only, and to make only authorized disclosures of this information.

272. The Notice Letter mailed by Defendant notified Plaintiff Toles that Defendant's network had been accessed and that Plaintiff's Private Information was involved in the Data Breach.

273. Furthermore, Defendant's Notice Letter directed Plaintiff Toles to be vigilant and to take certain steps to protect his Private Information and otherwise mitigate his damages.

274. As a result of the Data Breach, Plaintiff heeded Defendant's warnings and spent time dealing with the consequences of the Data Breach, which included time spent verifying the legitimacy of the Notice Letter and self-monitoring their accounts and credit reports to ensure no fraudulent activity had occurred. This time has been lost forever and cannot be recaptured.

275. Plaintiff Toles further suffered actual injury in the form of incurring an unauthorized charge of $1,700 to his Navy Federal checking account on or around September 2023. Plaintiff Toles is informed and believes that the unauthorized actor obtained access to his accounts as a direct result of the Data Breach. Plaintiff Toles' has yet to be reimbursed for this unauthorized charge. Plaintiff Toles spent time investigating and disputing (to no avail) this unauthorized charge, and has lost $1,700 of his money. Plaintiff Toles' account was thereafter closed.

276. Plaintiff Toles suffered actual injury in the form of damages to and diminution in the value of his Private Information —a form of intangible property that Plaintiff Toles entrusted to Defendant, which was compromised in and because of the Data Breach.

277. Plaintiff Toles suffered lost time, annoyance, interference, and inconvenience because of the Data Breach and has anxiety and increased concerns for the loss of privacy, as well as anxiety over the impact of cybercriminals accessing, using, and selling Plaintiff Toles' Private Information.

278. Plaintiff Toles suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from his Private Information, in combination with his name, being placed in the hands of unauthorized third parties/criminals.

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

Plaintiff Morgan

280. Plaintiff Morgan has utilized Defendant's services in the past.

281. Plaintiff Morgan was required to provide her Private Information to Defendant, including her name, demographic information, Social Security number and PHI.

282. At the time of the Data Breach, Defendant retained Plaintiff Morgan's Private Information in its system.

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

284. Plaintiff Morgan received the Notice Letter, by U.S. mail, from Defendant. According to the Notice Letter, Plaintiff's Private Information was improperly accessed and obtained by unauthorized third parties.

285. As a result of the Data Breach, and at the direction of Defendant's Notice Letter, Plaintiff Morgan made reasonable efforts to mitigate the impact of the Data Breach, including

considering cancelling payment cards, changing passwords and resecuring her own computer network, and checking her financial and credit accounts for any indication of fraudulent activity, which may take years to detect. 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.

286. Plaintiff Morgan further suffered actual injury. Upon information and belief, her Private Information is now on the dark web as a result of the Data Breach. In addition, she has experienced an increase in spam, which, upon information and belief, was caused by the Data Breach and began following the Data Breach.

287. The Data Breach has caused Plaintiff Morgan 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.

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

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

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

Plaintiff Autry

291. In order to receive pharmaceutical services, Defendant required Plaintiff Autry provide it with substantial amounts of his Private Information.

292. On October 30, 2023, Plaintiff Autry received a Notice Letter, which stated that Plaintiff Autry's name and prescription information may have been accessed in the Data Breach.

293. The confidentiality of Plaintiff Autry's sensitive information has been irreparably harmed. For the rest of his life, Plaintiff Autry will have to worry about when and how his sensitive information may be shared or used to his detriment.

294. As a result of the Data Breach, Plaintiff Autry spent time dealing with the consequences of the Data Breach, which includes times spent verifying the legitimacy of the Notice Letter and self-monitoring his accounts.

295. Plaintiff Autry is very careful about not sharing his sensitive Private Information. He has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source

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

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

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

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

Plaintiff Phillips

300. In order to receive pharmaceutical services, Defendant required Plaintiff Phillips to provide it with substantial amounts of her Private Information.

301. On October 30, 2023, Plaintiff Phillips received a Notice Letter, which stated that Plaintiff Phillips' name and prescription information were compromised in the Data Breach.

302. As a result of the Data Breach, the confidentiality of Plaintiff Phillips' sensitive information has been irreparably harmed. For the rest of her life, Plaintiff Phillips will have to worry about when and how her sensitive information may be shared or used to her detriment.

303. As a result of the Data Breach, Plaintiff Phillips spent time dealing with the consequences of the Data Breach, which includes times spent verifying the legitimacy of the Notice Letter and self-monitoring her accounts.

304. Plaintiff Phillips is very careful about not sharing her sensitive Private Information. She has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source

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

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

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

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

Plaintiff Hallman

309. Plaintiff Hallman is an adult individual and, at all relevant times herein, a resident and citizen of South Carolina. Plaintiff Hallman is a victim of the Data Breach.

310. Plaintiff Hallman was a direct client or a client of a business serviced by Defendant, and her information was stored with Defendant as a result of her dealings with Defendant.

311. As required in order to obtain services from Defendant, Plaintiff Hallman provided Defendant with highly sensitive personal information, who then possessed and controlled it.

312. As a result, Plaintiff Hallman's information was among the data accessed by an unauthorized third-party in the Data Breach.

313. Plaintiff Hallman received a Notice Letter from Defendant, dated October 31, 2023, stating that her Private Information was involved in the Data Breach.

314. As a result, Plaintiff Hallman was injured in the form of lost time dealing with the consequences of the Data Breach, which included and continues to include: time spent verifying the legitimacy and impact of the Data Breach; time spent exploring credit monitoring and identity theft insurance options; time spent self-monitoring her accounts with heightened scrutiny and time spent seeking legal counsel regarding her options for remedying and/or mitigating the effects of the Data Breach.

315. Plaintiff Hallman was also injured by the material risk to future harm she suffers based on Defendant's breach; this risk is imminent and substantial because Plaintiff Hallman's data has been exposed in the Breach, the data involved, including healthcare information, is highly sensitive and presents a high risk of identity theft or fraud; and it is likely, given Defendant's clientele, that some of the Class's information that has been exposed has already been misused.

316. Plaintiff Hallman suffered actual injury in the form of damages to and diminution in the value of her Private Information—a condition of intangible property that they entrusted to Defendant, which was compromised in and as a result of the Data Breach.

317. Plaintiff Hallman, as a result of the Data Breach, has increased anxiety for her loss of privacy and anxiety over the impact of cybercriminals accessing, using, and selling her Private Information.

318. Plaintiff Hallman has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from her Private

Information, in combination with her name, being placed in the hands of unauthorized third parties/criminals.

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

Plaintiff Fisher

320. Plaintiff Fisher was a direct client or a client of a business serviced by Defendant, and his information was stored with Defendant as a result of his dealings with Defendant.

321. As required in order to obtain services from Defendant, Plaintiff Fisher provided Defendant with highly sensitive personal information, who then possessed and controlled it.

322. As a result, Plaintiff Fisher's information was among the data accessed by an unauthorized third-party in the Data Breach.

323. Plaintiff Fisher received a Notice Letter from Defendant, dated October 31, 2023, stating that his Private Information was involved in the Data Breach.

324. As a result, Plaintiff Fisher was injured in the form of lost time dealing with the consequences of the Data Breach, which included and continues to include: time spent verifying the legitimacy and impact of the Data Breach; time spent exploring credit monitoring and identity theft insurance options; time spent self-monitoring his accounts with heightened scrutiny and time spent seeking legal counsel regarding his options for remedying and/or mitigating the effects of the Data Breach.

325. Plaintiff Fisher was also injured by the material risk to future harm he suffers based on Defendant's Breach; this risk is imminent and substantial because Plaintiff Fisher's data has been exposed in the Breach, the data involved, including healthcare information, is highly sensitive and presents a high risk of identity theft or fraud; and it is likely, given Defendant's clientele, that some of the Class's information that has been exposed has already been misused.

326. Plaintiff Fisher suffered actual injury in the form of damages to and diminution in the value of his Private Information—a condition of intangible property that they entrusted to Defendant, which was compromised in and as a result of the Data Breach.

327. Plaintiff Fisher, as a result of the Data Breach, has increased anxiety for his loss of privacy and anxiety over the impact of cybercriminals accessing, using, and selling his Private Information.

328. Plaintiff Fisher has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from his Private Information, in combination with his name, being placed in the hands of unauthorized third parties/criminals.

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

Plaintiff Sauceda

330. Plaintiff Sauceda has utilized Defendant's services since 2019.

331. In order to receive pharmaceutical services, Defendant required Plaintiff Sauceda to provide it with substantial amounts of his Private Information, including his name, demographic information, and PHI.

332. At the time of the Data Breach, Defendant retained Plaintiff Sauceda's Private information in its system.

333. Plaintiff Sauceda is very careful about sharing and protecting his Private Information. Plaintiff stores any documents containing his Private Information in a safe and secure location. He has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source. Plaintiff would not have entrusted his Private Information to Defendant had he known of Defendant's lax data security policies.

334. Plaintiff Sauceda received the Notice Letter, by U.S. mail, from Defendant. According to the Notice Letter, Plaintiff's Private Information was improperly accessed and obtained by unauthorized third parties.

335. The Notice Letter declined to offer Plaintiff Sauceda any complimentary credit monitoring services. Failing to offer credit monitoring is unacceptable given that Plaintiff Sauceda will now experience a lifetime of increased risk of identity theft including but not limited to potential medical fraud.

336. Plaintiff Sauceda suffered actual injury in the form of time spent dealing with the Data Breach and the increased risk of fraud resulting from the Data Breach and/or monitoring his accounts for fraud.

337. Plaintiff Sauceda suffered actual injury in the form of having his Private Information compromised and/or stolen as a result of the Data Breach.

338. The Data Breach has caused Plaintiff Sauceda to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendant has still not fully informed him of key details about the Data Breach's occurrence.

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

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

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

Plaintiff Lowery

342. Plaintiff Lowery has utilized Defendant's services in the past.

343. Plaintiff Lowery was required to provide his Private Information to Defendant, including his name, demographic information, Social Security number and PHI.

344. At the time of the Data Breach, Defendant retained Plaintiff Lowery's Private Information in its system.

345. Plaintiff Lowery is very careful about sharing and protecting his Private Information. Plaintiff stores any documents containing his Private Information in a safe and secure location. He has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source. Plaintiff would not have entrusted his Private Information to Defendant had he known of Defendant's lax data security policies.

346. Plaintiff Lowery received the Notice Letter, by U.S. mail, from Defendant. According to the Notice Letter, Plaintiff's Private Information was improperly accessed and obtained by unauthorized third parties.

347. The Notice Letter offered Plaintiff Lowery limited credit monitoring services, but such services are insufficient given that Plaintiff Lowery will now experience a lifetime of increased risk of identity theft, including but not limited to, potential medical fraud.

348. Plaintiff Lowery suffered actual injury in the form of time spent dealing with the Data Breach and the increased risk of fraud resulting from the Data Breach and/or monitoring his accounts for fraud.

349. The Data Breach has caused Plaintiff Lowery to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendant has still not fully informed him of key details about the Data Breach's occurrence.

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

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

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

Plaintiff Evans

353. Plaintiff Evans is not associated with PostMeds and is unsure how they acquired his information.

354. Plaintiff Evans received a Notice Letter from Defendant, in or around November 2023, stating that his Private Information was involved in the Data Breach, including his name, demographic information, and PHI.

355. At the time of the Data Breach, Defendant retained Plaintiff Evans' Private Information in its system.

356. Plaintiff Evans is very careful about sharing and protecting his Private Information. Plaintiff stores any documents containing his Private Information in a safe and secure location. He has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source. Plaintiff would not have entrusted his Private Information to Defendant had he known of Defendant's lax data security policies.

357. Plaintiff Evans received the Notice Letter, by U.S. mail, from Defendant. According to the Notice Letter, Plaintiff's Private Information was improperly accessed and obtained by unauthorized third parties.

358. Plaintiff Evans suffered actual injury in the form of time spent dealing with the Data Breach and the increased risk of fraud resulting from the Data Breach and/or monitoring his accounts for fraud. This time has been lost forever and cannot be recaptured.

359. Plaintiff Evans suffered actual injury in the form of having his Private Information compromised and/or stolen as a result of the Data Breach.

360. Plaintiff Evans suffered actual injury in the form of damages to and diminution in the value of his personal, health, and financial information – a form of intangible property that Plaintiff Evans entrusted to Defendant for the purpose of receiving healthcare services from Defendant and which was compromised in, and as a result of, the Data Breach.

361. The Data Breach has caused Plaintiff Evans to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendant has still not fully informed him of key details about the Data Breach's occurrence.

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

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

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

CLASS ACTION ALLEGATIONS

365. This action is properly maintainable as a class action. Plaintiffs bring this class action on behalf of themselves and on behalf of all others similarly situated.

366. Plaintiffs propose the following Class definition, subject to amendment as appropriate:

> **Nationwide Class**
> All individuals residing in the United States whose Private Information was compromised in the Data Breach announced by Defendant in October 2023, including all those who were sent a Notice Letter (the "Class").

367. Plaintiffs McDonald, Williams, Benjamin, and Garcia also seek to represent a California Subclass defined as:

> **California Subclass**
> All individuals residing in the State of California whose Private Information was compromised in the Data Breach announced by Defendant in October 2023, including all those who were sent a Notice Letter (the "California Subclass").

368. Plaintiff Siegel also seeks to represent an Illinois Subclass defined as:

Illinois Subclass
All individuals residing in the State of Illinois whose Private Information was compromised in the Data Breach announced by Defendant in October 2023, including all those who were sent a Notice Letter (the "Illinois Subclass").

369. Excluded from the Class and Subclasses (Collectively, the "Class") are the following individuals and/or entities: Defendant and Defendant's parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendant has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

370. Numerosity: The members of the Class are so numerous that joinder of all members is impracticable, if not completely impossible. Although the precise number of persons impacted in the Data Breach is currently unknown to Plaintiffs and exclusively in the possession of Defendant, upon information and belief, hundreds of thousands of persons were impacted in the Data Breach. The Class is apparently identifiable within Defendant's records, and Defendant has already identified these individuals (as evidenced by sending them Breach notification letters).

371. Common questions of law and fact exist as to all members of the Class that predominate over any questions affecting solely individual members of the Class. The questions of law and fact common to the Class, which may affect individual Class members, include, but are not limited to, the following:

a. Whether and to what extent Defendant had a duty to protect the Private Information of Plaintiffs and Class Members;

b. Whether Defendant had respective duties not to disclose the Private Information of Plaintiffs and Class Members to unauthorized third parties;

c. Whether Defendant had respective duties not to use the Private Information of Plaintiffs and Class Members for non-business purposes;

d. Whether Defendant failed to adequately safeguard the Private Information of Plaintiffs and Class Members;

e. Whether and when Defendant actually learned of the Data Breach;

f. Whether Defendant adequately, promptly, and accurately informed Plaintiffs and Class Members that their Private Information had been compromised;

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

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

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

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

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

372. Typicality: Plaintiffs' claims are typical of those of the other members of the Class because Plaintiffs, like every other Class Member, were exposed to virtually identical conduct and now suffer from the same violations of the law as each other member of the Class.

373. Policies Generally Applicable to the Class: This class action is also appropriate for certification because Defendant acted or refused to act on grounds generally applicable to the Class, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members and making final injunctive relief appropriate with respect to the Nationwide Class as a whole. Defendant's policies challenged herein apply to and affect Class Members uniformly and Plaintiffs' challenge of these policies hinges on Defendant's conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiffs.

374. Adequacy: Plaintiffs will fairly and adequately represent and protect the interests of the Class Members in that they have no disabling conflicts of interest that would be antagonistic to those of the other Class Members. Plaintiffs seek no relief that is antagonistic or adverse to the Class Members and the infringement of the rights and the damages they have suffered are typical of other Class Members. Plaintiffs have retained counsel experienced in complex class action and data breach litigation, and Plaintiffs intend to prosecute this action vigorously.

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

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

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

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

379. Unless a Class-wide injunction is issued, Defendant may continue in its failure to properly secure the Private Information of Class Members, Defendant may continue to refuse to provide proper notification to Class Members regarding the Data Breach, and Defendant may continue to act unlawfully as set forth in this Complaint.

380. Further, Defendant has acted or refused to act on grounds generally applicable to the Class and, accordingly, final injunctive or corresponding declaratory relief with regard to the Class Members as a whole is appropriate.

COUNT I
Negligence
(On Behalf of Plaintiffs and the Nationwide Class)

381. Plaintiffs restate and reallege the factual allegations set forth in paragraphs 1 through 364 as if fully alleged herein.

382. Defendant required Plaintiffs and Class Members to submit non-public Private Information as a condition of obtaining services at PostMeds.

383. Plaintiffs and Class Members entrusted their Private Information to Defendant with the understanding that Defendant would safeguard their Private Information and delete it once the relationship terminated.

384. By assuming the responsibility to collect and store this Private Information, 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 safeguard their computer property—and Class Members' Private Information held within it—to prevent disclosure of the Private Information, and to safeguard the Private Information from theft. Defendant's duty included a responsibility to

implement processes by which they could detect a breach of its security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a data breach.

385. 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.

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

387. 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 Private Information.

388. Defendant breached its duties, and thus was negligent, by failing to use reasonable measures to protect Class Members' Private Information. 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 Class Members' Private Information;

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

c. Failing to periodically ensure that their email system had plans in place to maintain reasonable data security safeguards;

d. Allowing unauthorized access to Class Members' Private Information; and,

e. Failing to detect in a timely manner that Class Members' Private Information had been compromised.

389. Defendant violated Section 5 of the FTC Act and HIPAA by failing to use reasonable measures to protect Private Information and not complying with applicable industry standards, as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of Private Information it obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiffs and the Class.

390. Plaintiffs and the Class are within the class of persons that the FTC Act and HIPAA were intended to protect.

391. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act and HIPAA were intended to guard against.

392. Defendant's violation of Section 5 of the FTC Act and HIPAA constitutes negligence.

393. 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 Plaintiffs and the Class.

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

395. It was foreseeable that Defendant's failure to use reasonable measures to protect Class Members' Private Information 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 pharmaceutical industry.

396. Defendant has full knowledge of the sensitivity of the Private Information and the types of harm that Plaintiffs and the Class could and would suffer if the Private Information were wrongfully disclosed.

397. Plaintiffs 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 Private Information of Plaintiffs and the Class, the

critical importance of providing adequate security of that Private Information, and the necessity for encrypting Private Information stored on Defendant's systems.

398. It was therefore foreseeable that the failure to adequately safeguard Class Members' Private Information would result in one or more types of injuries to Class Members.

399. Plaintiffs and the Class had no ability to protect their Private Information that was in, and possibly remains in, Defendant's possession.

400. Defendant was in an exclusive position to protect against the harm suffered by Plaintiffs and the Class as a result of the Data Breach.

401. Defendant's duty extended to protecting Plaintiffs 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.

402. Defendant has admitted that the Private Information of Plaintiffs and the Class was wrongfully lost and disclosed to unauthorized third persons as a result of the Data Breach.

403. But for Defendant's wrongful and negligent breach of duties owed to Plaintiffs and the Class, the Private Information of Plaintiffs and the Class would not have been compromised.

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

405. As a direct and proximate result of Defendant's negligence, Plaintiffs and the Class have suffered and will suffer injury, including but not limited to: (i) invasion of privacy;

(ii) theft of their Private Information; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) statutory damages; (viii) nominal damages; and (ix) the continued and certainly increased risk to their Private Information, 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 Private Information.

406. As a direct and proximate result of Defendant's negligence, Plaintiffs 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.

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

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

409. Defendant's negligent conduct is ongoing, in that it still holds the Private Information of Plaintiffs and Class Members in an unsafe and insecure manner.

410. Plaintiffs 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 Plaintiffs and the Nationwide Class)

411. Plaintiffs restate and reallege the factual allegations set forth in paragraphs 1 through 364 as if fully alleged herein.

412. Plaintiffs and Class Members were required to provide their Private Information to Defendant as a condition of obtaining services from Defendant.

413. Plaintiffs and Class Members provided their Private Information to Defendant in exchange for (among other things) Defendant's promise to protect their Private Information from unauthorized disclosure and to delete it once it was no longer necessary to maintain the Private Information for business purposes. Defendant additionally promulgated, adopted, and implemented written privacy policies whereby it expressly promised Plaintiffs and Class Members that it would only disclose Private Information under certain circumstances, none of which relate to the Data Breach.

414. On information and belief, Defendant further promised to and represented it would comply with industry standards and to make sure that Plaintiffs' and Class Members' Private Information would remain protected.

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

416. When Plaintiffs and Class Members provided their Private Information to Defendant as a condition of obtaining services at Defendant, they entered into implied contracts with Defendant pursuant to which Defendant agreed to reasonably protect such information.

417. Defendant required Class Members to provide their Private Information as part of Defendant's regular business practices. Plaintiffs and Class Members accepted Defendant's offers and provided their Private Information to Defendant.

418. In entering into such implied contracts, Plaintiffs 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.

419. Plaintiffs and Class Members would not have entrusted their Private Information to Defendant in the absence of the implied contract between them and Defendant to keep their information reasonably secure.

420. Plaintiffs and Class Members would not have entrusted their Private Information to Defendant in the absence of its implied promise to monitor its computer systems and networks to ensure that it adopted reasonable data security measures.

421. Plaintiffs and Class Members fully and adequately performed their obligations under the implied contracts with Defendant.

422. Defendant breached its implied contracts with Plaintiffs and Class Members by failing to safeguard and protect their Private Information.

423. As a direct and proximate result of Defendant's breaches of the implied contracts, Plaintiffs and Class Members sustained damages as alleged herein.

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

425. Plaintiffs and Class Members are also entitled to nominal damages for the breach of implied contract.

426. Plaintiffs and Class Members are also entitled to injunctive relief requiring Defendant to, e.g., (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit monitoring to the Class.

COUNT III
Unjust Enrichment / Quasi Contract
(On Behalf of Plaintiffs and the Nationwide Class)

427. Plaintiffs restate and reallege the factual allegations set forth in paragraphs 1 through 364 as if fully alleged herein.

428. This Count is pleaded in the alternative to the breach of implied contract claim (Count II) above.

429. Plaintiffs and Class Members conferred a monetary benefit upon Defendant by providing payments to Defendant as well as by providing their valuable Private Information to Defendant.

430. Plaintiffs and Class Members provided Defendant their Private Information on the understanding that Defendant would pay for the administrative costs of reasonable data privacy and security practices and procedures from the revenue it derived therefrom. In exchange, Plaintiffs and Class Members should have received adequate protection and data security for such Private Information held by Defendant.

431. Defendant benefited from receiving Plaintiffs' and Class Members' payments for services, whether directly or indirectly, and from receiving their Private Information through its ability to retain and use that information for its own benefit. Defendant understood and accepted this benefit.

432. Defendant knew Plaintiffs and Class members conferred a benefit which Defendant accepted. Defendant profited from these transactions and used the Private Information of Plaintiffs and Class Members for business purposes.

433. Because all Private Information provided by Plaintiffs and Class Members was similarly at risk from a foreseeable and targeted data breach, Defendant's obligation to safeguard the Private Information it collected from its customers was inherent to the relationship.

434. Defendant also understood and appreciated that Plaintiffs' and Class Members' Private Information was private and confidential, and its value depended upon Defendant maintaining the privacy and confidentiality of that information.

435. Defendant failed to provide reasonable security, safeguards, and protections to the Private Information of Plaintiffs and Class Members.

436. Defendant enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiffs' and Class Members' Private Information.

437. Instead of providing a reasonable level of security that would have prevented the Data Breach, Defendant instead made calculated decisions to avoid its data security obligations at the expense of Plaintiffs and Class Members by utilizing cheaper, ineffective security measures. Plaintiffs and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's failure to provide the requisite security.

438. Under the principles of equity and good conscience, Defendant should not be permitted to retain money belonging to Plaintiffs and Class Members, because Defendant failed to implement appropriate data management and security measures mandated by industry standards.

439. Defendant's enrichment at the expense of Plaintiffs and Class Members is and was unjust.

440. Defendant acquired the monetary benefit and Private Information through inequitable means in that they failed to disclose the inadequate security practices previously alleged.

441. If Plaintiffs and Class Members knew that Defendant had not secured their Private Information, they would not have agreed to provide their Private Information to Defendant.

442. Plaintiffs and Class Members have no adequate remedy at law.

443. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have suffered and will suffer injury as described herein.

444. Plaintiffs and the Class Members are entitled to restitution and disgorgement of all profits, benefits, and other compensation obtained by Defendant, plus attorneys' fees, costs, and interest thereon.

COUNT IV
Invasion of Privacy – Intrusion Upon Seclusion
(On behalf of Plaintiffs and the Nationwide Class)

445. Plaintiffs restate and reallege the factual allegations set forth in paragraphs 1 through 364 as if fully alleged herein.

446. To assert claims for intrusion upon seclusion, one must plead (1) that the defendant intentionally intruded into a matter as to which plaintiff had a reasonable expectation of privacy; and (2) that the intrusion was highly offensive to a reasonable person.

447. PostMeds intentionally intruded upon the solitude, seclusion and private affairs of Plaintiffs and Class Members by intentionally configuring their systems in such a way that left them vulnerable to malware/ransomware attack, thus permitting unauthorized access to their systems, which compromised Plaintiffs' and Class Members' personal information. Only PostMeds had control over its systems.

448. PostMeds' conduct is especially egregious and offensive as they failed to have adequate security measures in place to prevent, track, or detect in a timely fashion unauthorized access to Plaintiffs' and Class Members' personal information.

449. At all times, PostMeds was aware that Plaintiffs' and Class Members' personal information in their possession contained highly sensitive and confidential personal information.

450. Plaintiffs and Class Members have a reasonable expectation of privacy in their personal information, which also contains highly sensitive medical information.

451. PostMeds intentionally configured their systems in such a way that stored Plaintiffs' and Class Members' personal information to be left vulnerable to malware/ransomware attack without regard for Plaintiffs' and Class Members' privacy interests.

452. The disclosure of the sensitive and confidential personal information of thousands of consumers, was highly offensive to Plaintiffs and Class Members because it violated expectations of privacy that have been established by general social norms, including by granting access to information and data that is private and would not otherwise be disclosed.

453. PostMeds' conduct would be highly offensive to a reasonable person in that it violated statutory and regulatory protections designed to protect highly sensitive information, in addition to social norms. PostMeds' conduct would be especially egregious to a reasonable person as PostMeds publicly disclosed Plaintiffs' and Class Members' sensitive and confidential personal information without their consent, to an "unauthorized person," i.e., hackers.

454. As a result of PostMeds' actions, Plaintiffs and Class Members have suffered harm and injury, including but not limited to an invasion of their privacy rights.

455. Plaintiffs and Class Members have been damaged as a direct and proximate result of PostMeds' intrusion upon seclusion and are entitled to just compensation.

456. Plaintiffs and Class Members are entitled to appropriate relief, including compensatory damages for the harm to their privacy, loss of valuable rights and protections, and heightened stress, fear, anxiety and risk of future invasions of privacy.

COUNT V
Violation of the California Unfair Competition Law,
Cal. Bus. & Prof. Code §17200 *et seq.*
(On Behalf of Plaintiffs and the Nationwide Class)

457. Plaintiffs restate and reallege the factual allegations set forth in paragraphs 1 through 364 as if fully alleged herein.

458. Defendant is a "person" defined by Cal. Bus. & Prof. Code § 17201.

459. Defendant violated Cal. Bus. & Prof. Code § 17200 et seq. ("UCL") by engaging in unlawful, unfair, and deceptive business acts and practices.

460. Defendant's violations of the UCL were prepared, directed, and emanated from Defendant's California headquarters and from where it maintains its principal corporate offices in California.

461. Defendant's "unfair" acts and practices include:

a. Defendant failed to implement and maintain reasonable security measures to protect Plaintiffs' and Class Members' personal information from unauthorized disclosure, release, data breaches, and theft, which was a direct and proximate

cause of the Defendant Data Breach. Defendant failed to identify foreseeable security risks, remediate identified security risks, and adequately improve security following previous cybersecurity incidents and known coding vulnerabilities in the industry;

b. Defendant's failure to implement and maintain reasonable security measures also was contrary to legislatively-declared public policy that seeks to protect consumers' data and ensure that entities that are trusted with it use appropriate security measures. These policies are reflected in laws, including HIPAA, the FTC Act (15 U.S.C. § 45), California's Customer Records Act (Cal. Civ. Code § 1798.80 et seq.), and California's Consumer Privacy Act (Cal. Civ. Code § 1798.150);

c. Defendant's failure to implement and maintain reasonable security measures also led to substantial consumer injuries, as described above, that are not outweighed by any countervailing benefits to consumers or competition. Moreover, because consumers could not know of Defendant's inadequate security, consumers could not have reasonably avoided the harms that Defendant caused; and

d. Engaging in unlawful business practices by violating Cal. Civ. Code § 1798.82.

462. Defendant has engaged in "unlawful" business practices by violating multiple laws, including HIPAA, the FTC Act, 15 U.S.C. § 45, and California common law.

463. Defendant's unlawful, unfair, and deceptive acts and practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs' and Class Members' personal information, which was a direct and proximate cause of the Defendant Data Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, which was a direct and proximate cause of the Defendant Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Class Members' personal information, including duties imposed by HIPAA and the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Defendant Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiffs' and Class Members' personal information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Class Members' personal information, including duties imposed by HIPAA and the FTC Act, 15 U.S.C. § 45;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiffs' and Class Members' personal information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Class Members' personal information, including duties imposed by HIPAA and the FTC Act, 15 U.S.C. § 45.

464. Defendant's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendant's data security and ability to protect the confidentiality of consumers' personal information.

465. As a direct and proximate result of Defendant's unfair, unlawful, and fraudulent acts and practices, Plaintiffs and Class Members' were injured and lost money or property, which would not have occurred but for the unfair and deceptive acts, practices, and omissions alleged herein, time and expenses related to monitoring their financial accounts for fraudulent activity, an increased, imminent risk of fraud and identity theft, and loss of value of their personal information.

466. Defendant's violations were, and are, willful, deceptive, unfair, and unconscionable.

467. Plaintiffs and Class Members have lost money and property as a result of Defendant's conduct in violation of the UCL, as stated herein and above.

468. By deceptively storing, collecting, and disclosing their personal information, Defendant has taken money or property from Plaintiffs and Class Members. Had Plaintiffs known that Defendant would fail to implement reasonable data security polices they would not have provided their personal information to Defendant.

469. Defendant acted intentionally, knowingly, and maliciously to violate California's Unfair Competition Law, and recklessly disregarded Plaintiffs' and Class Members' rights.

470. Plaintiffs and Class Members seek all monetary and nonmonetary relief allowed by law, including restitution of all profits stemming from Defendant's unfair, unlawful, and fraudulent business practices or use of their personal information; declaratory relief; reasonable attorneys' fees and costs under California Code of Civil Procedure § 1021.5; injunctive relief; and other appropriate equitable relief, including public injunctive relief.

COUNT VI
Violation of the California Confidentiality of Medical Information Act ("CMIA"), Cal. Civ. Code § 56, *et seq.*
(On behalf of California Plaintiffs and the California Class)

471. Plaintiffs McDonald, Williams, Benjamin, Sauceda, and Garcia ("Plaintiffs" for the purposes of this Count) restate and reallege the factual allegations set forth in paragraphs 1 through 364 as if fully alleged herein.

472. Plaintiffs allege this Count on their own behalf and on behalf of the California Subclass (the "Class" for the purposes of this Count).

473. Section 56.10(a) of the California Civil Code provides that "[a] provider of health care, health care service plan, or contractor shall not disclose medical information regarding a patient of the provider of health care or an enrollee or subscriber of a health care service plan without first obtaining an authorization[.]"

474. PostMeds is a "contractor" within the meaning of Civil Code § 56.05(d) within the meaning of Civil Code § 56.06 and/or a "business organized for the purpose of maintaining medical information" and/or a "business that offers software or hardware to consumers . . . that is designed to maintain medical information" within the meaning of Civil Code § 56.06(a) and (b), and maintained and continues to maintain "medical information," within the meaning of Civil Code § 56.05(j), for "patients" of PostMeds, within the meaning of Civil Code § 56.05(k).

475. Plaintiffs and Class Members are "patients" within the meaning of Civil Code § 56.05(k) and are "endanger[ed]" within the meaning of Civil Code § 56.05(e) because Plaintiffs and Class members fear that disclosure of their medical information could subject them to harassment or abuse.

476. Plaintiffs and Class Members, as patients, had their individually identifiable "medical information," within the meaning of Civil Code § 56.05(j), created, maintained, preserved, and stored on PostMeds' computer network at the time of the unauthorized disclosure.

477. PostMeds, through inadequate security, allowed unauthorized third-party access to Plaintiffs' and Class Members' medical information, without the prior written authorization of Plaintiffs and Class Members, as required by Civil Code § 56.10 of the CMIA.

478. In violation of Civil Code § 56.10(a), PostMeds disclosed Plaintiffs' and Class Members' medical information without first obtaining an authorization. Plaintiffs' and Class Members' medical information was viewed by unauthorized individuals as a direct and proximate result of PostMeds' violation of Civil Code § 56.10(a).

479. In violation of Civil Code § 56.10(e), PostMeds further disclosed Plaintiffs' and Class Members' medical information to persons or entities not engaged in providing direct health care services to Plaintiffs or Class Members, or to their providers of health care or health care service plans or their insurers or self-insured employers.

480. PostMeds violated Civil Code § 56.101 of the CMIA through its willful and knowing failure to maintain and preserve the confidentiality of the medical information of Plaintiffs and the Class Members. PostMeds' conduct with respect to the disclosure of

confidential Private Information was willful and knowing because PostMeds designed and implemented the computer network and security practices that gave rise to the unlawful disclosure.

481. In violation of Civil Code § 56.101(a), PostMeds created, maintained, preserved, stored, abandoned, destroyed, or disposed of Plaintiffs' and Class Members' medical information in a manner that failed to preserve and breached the confidentiality of the information contained therein. Plaintiffs' and Class Members' medical information was viewed by unauthorized individuals as a direct and proximate result of PostMeds' violation of Civil Code § 56.101(a).

380. In violation of Civil Code § 56.101(a), PostMeds negligently created, maintained, preserved, stored, abandoned, destroyed, or disposed of Plaintiffs' and Class Members' medical information. Plaintiffs' and Class Members' medical information was viewed by unauthorized individuals as a direct and proximate result of PostMeds' violation of Civil Code § 56.101(a).

482. Plaintiffs' and Class Members' medical information that was the subject of the unauthorized disclosure included "electronic medical records" or "electronic health records" as referenced by Civil Code § 56.101(c) and defined by 42 U.S.C. § 17921(5).

483. In violation of Civil Code § 56.101(b)(1)(A), PostMeds' electronic health record system or electronic medical record system failed to protect and preserve the integrity of electronic medical information. Plaintiffs' and Class Members' medical information was viewed by unauthorized individuals as a direct and proximate result of PostMeds' violation of Civil Code § 56.101(b)(1)(A).

484. PostMeds violated Civil Code § 56.36 of the CMIA through its failure to maintain and preserve the confidentiality of the medical information of Plaintiffs and the Class Members.

485. As a result of PostMeds' above-described conduct, Plaintiffs and Class Members have suffered damages from the unauthorized disclosure and release of their individual identifiable "medical information" made unlawful by Civil Code §§ 56.10, 56.101, 56.36. 385. As a direct and proximate result of PostMeds' above-described wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused the unauthorized

disclosure, and violation of the CMIA, Plaintiffs and Class Members have suffered (and will continue to suffer) economic damages and other injury and actual harm in the form of, inter alia, (i) an imminent, immediate and the continuing increased risk of identity theft, identity fraud and medical fraud-risks justifying expenditures for protective and remedial services for which they are entitled to compensation, (ii) invasion of privacy, (iii) breach of the confidentiality of their Private Information, (iv) statutory damages under the California CMIA, (v) deprivation of the value of their Private Information, for which there is a well-established national and international market, and/or (vi) the financial and temporal cost of monitoring their credit, monitoring their financial accounts, and mitigating their damages.

486. Plaintiffs, individually and for each member of the Class, seeks nominal damages of one thousand dollars ($1,000) for each violation under Civil Code § 56.36(b)(1), and actual damages suffered, if any, pursuant to Civil Code § 56.36(b)(2), injunctive relief, as well as punitive damages of up to $3,000 per Plaintiffs and each Class Member, and attorneys' fees, litigation expenses and court costs, pursuant to Civil Code § 56.35.

COUNT VII
Violation of the California Customer Records Act, Cal. Civ. Code §§ 1798.80 *et seq.*, (On Behalf of California Plaintiffs and the California Class)

487. Plaintiffs McDonald, Williams, Benjamin, Sauceda, and Garcia ("Plaintiffs" for the purposes of this Count) restate and reallege the factual allegations set forth in paragraphs 1 through 364 as if fully alleged herein.

488. Plaintiffs allege this Count on their own behalf and on behalf of the California Subclass (the "Class" for the purposes of this Count).

489. Cal. Civ. Code § 1798.81.5 provides that "[i]t is the intent of the Legislature to ensure that personal information about California residents is protected. To that end, the purpose of this section is to encourage businesses that own, license, or maintain personal information about Californians to provide reasonable security for that information."

490. Section 1798.81.5(b) further states that: "[a] business that owns, licenses, or maintains personal information about a California resident shall implement and maintain

reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure."

491. Cal. Civ. Code § 1798.84(b) provides that [a]ny customer injured by a violation of this title may institute a civil action to recover damages." Section 1798.84(e) further provides that "[a]ny business that violates, proposes to violate, or has violated this title may be enjoined."

492. Plaintiffs and members of the Class are "customers" within the meaning of Civ. Code § 1798.80(c) and 1798.84(b) because they are individuals who provided personal information to PostMeds, directly and/or indirectly, for the purpose of obtaining a service from PostMeds.

493. The personal information of Plaintiffs and the Class at issue in this lawsuit constitutes "personal information" under § 1798.81.5(d)(1) in that the personal information PostMeds collects and which was impacted by the cybersecurity attack includes an individual's first name or first initial and the individual's last name in combination with one or more of the following data elements, with either the name or the data elements not encrypted or redacted: (i) Social Security number; (ii) Driver's license number, California identification card number, tax identification number, passport number, military identification number, or other unique identification number issued on a government document commonly used to verify the identity of a specific individual; (iii) account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account; (iv) medical information; (v) health insurance information; (vi) unique biometric data generated from measurements or technical analysis of human body characteristics, such as a fingerprint, retina, or iris image, used to authenticate a specific individual.

494. PostMeds knew or should have known that its computer systems and data security practices were inadequate to safeguard the Class' personal information and that the risk of a data breach or theft was highly likely. PostMeds failed to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal

information of Plaintiffs and the Class. Specifically, PostMeds failed to implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information of Plaintiffs and the Class from unauthorized access, destruction, use, modification, or disclosure. PostMeds further subjected Plaintiffs' and the Class' nonencrypted and nonredacted personal information to an unauthorized access and exfiltration, theft, or disclosure as a result of the PostMeds' violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information, as described herein.

495. As a direct and proximate result of PostMeds' violation of its duty, the unauthorized access, destruction, use, modification, or disclosure of the personal information of Plaintiffs and the Class included hackers' access to, removal, deletion, destruction, use, modification, disabling, disclosure and/or conversion of the personal information of Plaintiffs and the Class by the ransomware attackers and/or additional unauthorized third parties to whom those cybercriminals sold and/or otherwise transmitted the information.

496. As a direct and proximate result of PostMeds' acts or omissions, Plaintiffs and the Class were injured and lost money or property including, but not limited to, the loss of Plaintiffs' and the subclass's legally protected interest in the confidentiality and privacy of their personal information, nominal damages, and additional losses described above. Plaintiffs seeks compensatory damages as well as injunctive relief pursuant to Cal. Civ. Code § 1798.84(b).

497. Moreover, the California Customer Records Act further provides: "A person or business that maintains computerized data that includes personal information that the person or business does not own shall notify the owner or licensee of the information of the breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person." Cal. Civ. Code § 1798.82.

498. Any person or business that is required to issue a security breach notification under the CRA must meet the following requirements under §1798.82(d):

a. The name and contact information of the reporting person or business subject to this section;

b. A list of the types of personal information that were or are reasonably believed to have been the subject of a breach;

c. If the information is possible to determine at the time the notice is provided, then any of the following:

i. the date of the breach,

ii. the estimated date of the breach, or

iii. the date range within which the breach occurred. The notification shall also include the date of the notice;

d. Whether notification was delayed as a result of a law enforcement investigation, if that information is possible to determine at the time the notice is provided;

e. A general description of the breach incident, if that information is possible to determine at the time the notice is provided;

f. The toll-free telephone numbers and addresses of the major credit reporting agencies if the breach exposed a social security number or a driver's license or California identification card number;

g. If the person or business providing the notification was the source of the breach, an offer to provide appropriate identity theft prevention and mitigation services, if any, shall be provided at no cost to the affected person for not less than 12 months along with all information necessary to take advantage of the offer to any person whose information was or may have been breached if the breach exposed or may have exposed personal information.

499. PostMeds failed to provide the legally compliant notice under § 1798.82(d) to Plaintiffs and members of the Class. On information and belief, to date, PostMeds has not sent written notice of the Data Breach to all impacted individuals. As a result, PostMeds has violated § 1798.82 by not providing legally compliant and timely notice to all Class Members. Because

not all members of the Class have been notified of the Breach, members could have taken action to protect their Private Information but were unable to do so because they were not timely notified of the Breach.

500. On information and belief, many Class Members affected by the Breach, have not received any notice at all from PostMeds in violation of Section 1798.82(d).

501. As a result of the violations of Cal. Civ. Code § 1798.82, Plaintiffs and Class Members suffered incrementally increased damages separate and distinct from those simply caused by the breaches themselves.

502. As a direct consequence of the actions as identified above, Plaintiffs and Class Members incurred additional losses and suffered further harm to their privacy, including but not limited to economic loss, the loss of control over the use of their identity, increased stress, fear, and anxiety, harm to their constitutional right to privacy, lost time dedicated to the investigation of the breach and effort to cure any resulting harm, the need for future expenses and time dedicated to the recovery and protection of further loss, and privacy injuries associated with having their sensitive personal, financial, and payroll information disclosed, that they would not have otherwise incurred, and are entitled to recover compensatory damages according to proof pursuant to § 1798.84(b).

COUNT VIII
Invasion of Privacy – Cal. Const. Art. 1, § 1
(On behalf of California Plaintiffs and the California Class)

503. Plaintiffs McDonald, Williams, Benjamin, Sauceda, and Garcia ("Plaintiffs" for the purposes of this Count) restate and reallege the factual allegations set forth in paragraphs 1 through 364 as if fully alleged herein.

504. Plaintiffs allege this Count on their own behalf and on behalf of the California Subclass (the "Class" for the purposes of this Count).

505. Art. I, § 1 of the California Constitution provides: "All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and

liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and privacy." Art. I, § 1, Cal. Const.

506. The right to privacy in California's constitution creates a private right of action against private and government entities.

507. To state a claim for invasion of privacy under the California Constitution, a plaintiff must establish: (1) a legally protected privacy interest; (2) a reasonable expectation of privacy; and (3) an intrusion so serious in nature, scope, and actual or potential impact as to constitute an egregious breach of the social norms.

508. PostMeds violated Plaintiffs' and Class Members' constitutional right to privacy by collecting, storing, and disclosing their personal information in which they had a legally protected privacy interest, and in which they had a reasonable expectation of privacy in, in a manner that was highly offensive to Plaintiffs and Class Members, would be highly offensive to a reasonable person, and was an egregious violation of social norms.

509. PostMeds has intruded upon Plaintiffs' and Class Members' legally protected privacy interests, including interests in precluding the dissemination or misuse of their confidential personal information.

510. PostMeds' actions constituted a serious invasion of privacy that would be highly offensive to a reasonable person in that: (i) the invasion occurred within a zone of privacy protected by the California Constitution, namely the misuse of information gathered for an improper purpose; and (ii) the invasion deprived Plaintiffs and Class Members of the ability to control the circulation of their personal information, which is considered fundamental to the right to privacy.

511. Plaintiffs and Class Members had a reasonable expectation of privacy in that: (i) PostMeds' invasion of privacy occurred as a result of PostMeds' security practices including the collecting, storage, and unauthorized disclosure of consumers' personal information; (ii) Plaintiffs and Class Members did not consent or otherwise authorize PostMeds to disclosure their

personal information; and (iii) Plaintiffs and Class Members could not reasonably expect PostMeds would commit acts in violation of laws protecting privacy.

512. As a result of PostMeds' actions, Plaintiffs and Class Members have been damaged as a direct and proximate result of PostMeds' invasion of their privacy and are entitled to just compensation.

513. Plaintiffs and Class Members suffered actual and concrete injury as a result of PostMeds' violations of their privacy interests. Plaintiffs and Class Members are entitled to appropriate relief, including damages to compensate them for the harm to their privacy interests, loss of valuable rights and protections, heightened stress, fear, anxiety, and risk of future invasions of privacy, and the mental and emotional distress and harm to human dignity interests caused by Defendant's invasions.

514. Plaintiffs and Class Members seek appropriate relief for that injury, including but not limited to damages that will reasonably compensate Plaintiffs and Class Members for the harm to their privacy interests as well as disgorgement of profits made by PostMeds as a result of its intrusions upon Plaintiffs' and Class Members' privacy.

COUNT IX
Violation of the Illinois Consumer Fraud and Deceptive Business Practices Act, 815 ILCS 505/2, *et seq*. ("ICFA")
(On Behalf of Plaintiff Siegel and the Illinois Class)

515. Plaintiff Siegel ("Plaintiff" for the purposes of this Count) restates and realleges the factual allegations set forth in paragraphs 1 through 364 as if fully alleged herein.

516. Plaintiff alleges this Count on his own behalf and on behalf of the Illinois Subclass (the "Class" for the purposes of this Count).

517. PostMeds offered and continues to offer pharmacy and other services in the State of Illinois.

518. Plaintiff and Class Members purchased and received pharmacy or other services or products from PostMeds for personal, family, or household purposes.

519. PostMeds engaged in unlawful and unfair practices in violation of the ICFA by failing to implement and maintain reasonable security measures to protect and secure its clients' Private Information in a manner that complied with applicable laws, regulations, and industry standards.

520. PostMeds makes explicit statements to its patients that their Private Information will remain private.

521. PostMeds' duties also arise from the Illinois Personal Information Protection Act, 815 ILCS 530/45(a) which requires:

a. A data collector that owns or licenses, or maintains or stores but does not own or license, records that contain personal information concerning an Illinois resident shall implement and maintain reasonable security measures to protect those records from unauthorized access, acquisition, destruction, use, modification, or disclosure.

815 ILCS 530/45. PostMeds violated this duty by failing to implement reasonably secure data security policies.

522. PostMeds further violated the ICFA by failing to notify its current and former patients of the Data Breach in a timely manner. The Illinois Personal Information Protection Act requires entities that experience a data breach to notify Illinois residents "in the most expedient time possible and without unreasonable delay." 815 ILCS 530/10. Violation of the Illinois Personal Information Protection Act constitutes an unlawful practice under the ICFA. 815 ILCS 530/20.

523. Due to the Data Breach, Plaintiff and Class members have lost property in the form of their Private Information. Further, PostMeds' failure to adopt reasonable practices in protecting and safeguarding its clients' Private Information will force Plaintiff and Class Members to spend time or money to protect against identity theft. Plaintiff and Class Members are now at a higher risk of medical identity theft and other crimes. This harm sufficiently

outweighs any justifications or motives for PostMeds' practice of collecting and storing Private Information without appropriate and reasonable safeguards to protect such information.

524. As a result of PostMeds' violations of the ICFA, Plaintiff and Class Members have suffered and will suffer injury, including, but not limited to: (i) a substantial increase in the likelihood of identity theft; (ii) the compromise, publication, and theft of their Private Information; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from unauthorized use of their Private Information; (iv) lost opportunity costs associated with effort attempting to mitigate the actual and future consequences of the Data Breach; (v) the continued risk to their Private Information which remains in PostMeds' possession; (vi) future costs in terms of time, effort, and money that will be required to prevent, detect, and repair the impact of the Private Information compromised as a result of the Data Breach; and (vii) overpayment for the services that were received without adequate data security.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs pray for judgment as follows:

A. For an Order certifying this action as a class action and appointing Plaintiffs and their counsel to represent the Class and Subclasses;

B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiffs' and Class Members' Private Information, and from refusing to issue prompt, complete and accurate disclosures to Plaintiffs 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 Private Information compromised during the Data Breach;

D. For injunctive relief requested by Plaintiffs, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiffs 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 Private Information of Plaintiffs 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 Plaintiffs and Class Members;

iv. Requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the Private Information of Plaintiffs and Class Members;

v. Prohibiting Defendant from maintaining the Private Information of Plaintiffs and Class Members on a cloud-based database;

vi. Requiring Defendant to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to

promptly correct any problems or issues detected by such third-party security auditors;

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

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

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

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

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

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

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

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

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

Plaintiffs demand a trial by jury on all claims so triable.

Dated: April 3, 2024

Respectfully submitted,

s/ Gary. M. Klinger

Gary. M. Klinger (*admitted pro hac vice*)
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
227 W. Monroe Street, Suite 2100
Chicago, Illinois 60606
Telephone: 866.252.0878
Email: gklinger@milberg.com

James J. Pizzirusso
(*admitted pro hac vice*)
Hausfeld LLP
888 16th Street, NW, Suite 300
Washington, DC 20006
Phone: (202) 542-7200
Fax: (202) 542-7201
Email: jpizzirusso@hausfeld.com

Plaintiffs' Interim Co-Lead Counsel

JILL M. MANNING (Bar No. 178849)
jmanning@pwfirm.com
PEARSON WARSHAW, LLP
555 Montgomery Street, Suite 1205
San Francisco, California 94111
Telephone: (415) 433-9000
Facsimile: (415) 433-9008

Plaintiffs' Interim Liaison Counsel

Attorneys for Plaintiffs and the Proposed Class