John J. Nelson (SBN 317598)
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, LLC
402 W. Broadway, Suite 1760
San Diego, CA 92101
Telephone: (858) 209-6941
Email: jnelson@milberg.com

Attorney for Plaintiff and the Proposed Class

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

RICHARD REED, individually and on behalf of all others similarly situated, Plaintiff, vs. POSTMEDS, INC. d/b/a TRUEPILL, Defendant.	Case No. _____ **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiff Richard Reed ("Plaintiff") brings this Class Action Complaint ("Complaint") against Defendant PostMeds, Inc. d/b/a TruePill ("PostMeds" or "Defendant") as an individual and on behalf of all others similarly situated, and alleges, upon personal knowledge as to his own actions and his 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. Plaintiff's 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. PostMeds collected and maintained certain personally identifiable information and protected health information of Plaintiff and the putative Class Members (defined below), who are (or were) customers at PostMeds.

5. The information compromised in the Data Breach included Plaintiff's and Class Members' full names, demographic information ("personally identifiable information" or "PII") and medical and health insurance information, 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 exfiltrated by cyber-criminals and remains in the hands of those cyber-criminals who target Private Information for its value to identity thieves.

7. As a result of the Data Breach, Plaintiff and Class Members, suffered concrete injuries in fact 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) Plaintiff experiencing suspicious activity on his

[1] https://www.truepill.com/ (last accessed Nov. 3, 2023).

Venmo account; (viii) Plaintiff's Private Information being disseminated on the dark web, according to CreditWise and Experian; (ix) experiencing an increase in spam calls, texts, and/or emails; (x) statutory damages; (xi) nominal damages; and (xii) 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.

8. 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 customers' Private Information from a foreseeable and preventable cyber-attack.

9. 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 Plaintiff's 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.

10. Defendant disregarded the rights of Plaintiff 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 Plaintiff and Class Members prompt and accurate notice of the Data Breach.

11. Plaintiff's 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.

12. 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.

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

14. Plaintiff 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.

15. Plaintiff brings 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 Plaintiff and other Class Members that their information had been subject to the unauthorized access by an unknown third party and precisely what specific type of information was accessed.

16. Through this Complaint, Plaintiff seeks to remedy these harms on behalf of himself and all similarly situated individuals whose Private Information was accessed during the

Data Breach.

17. Plaintiff seeks remedies including, but not limited to, compensatory damages and injunctive relief including improvements to Defendant's data security systems, future annual audits, and adequate credit monitoring services funded by Defendant.

PARTIES

18. Plaintiff, Richard Reed, is a natural person and resident of Charleston, West Virginia.

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

JURISDICTION AND VENUE

20. 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 Plaintiff, is a citizen of a state different from Defendant.

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

22. 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

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

24. Plaintiff and Class Members are current and former customers at PostMeds.

25. As a condition of obtaining services at PostMeds, Plaintiff and Class Members were required to provide their Private Information to Defendant.

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

27. Upon information and belief, in the course of collecting Private Information from its customers, including Plaintiff, Defendant promised to provide confidentiality and adequate security for customer data through its applicable privacy notice and through other disclosures in compliance with statutory privacy requirements.

28. 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]

29. Plaintiff 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.

30. Plaintiff and the Class Members have taken reasonable steps to maintain the

[2] https://www.truepill.com/ (last accessed Nov. 3, 2023).
[3] https://www.truepill.com/legal/nopp (last accessed Nov. 3, 2023).

confidentiality of their Private Information. Plaintiff 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. Plaintiff and Class Members value the confidentiality of their Private Information and demand security to safeguard their Private Information.

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

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

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

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

The Data Breach

35. On or about October 30, 2023, Defendant began sending Plaintiff 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]

36. 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 Plaintiff and Class Members, who retain a vested interest in ensuring that their Private Information remains protected.

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

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

39. The attacker accessed and acquired files Defendant shared with a third party containing unencrypted Private Information of Plaintiff and Class Members, including their PHI and other sensitive information. Plaintiff's and Class Members' Private Information was accessed and stolen in the Data Breach.

40. Plaintiff has already been informed that his Private Information has been disseminated on the dark web, and Plaintiff further believes that the Private Information of Class

[4] The "Notice Letter".

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

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

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

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

- Implement an awareness and training program. Because end users are targets, individuals should be aware of the threat of ransomware and how it is delivered.
- Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.
- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.
- Configure firewalls to block access to known malicious IP addresses.
- Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system.
- Set anti-virus and anti-malware programs to conduct regular scans automatically.

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

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

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

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

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

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

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

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

44. To prevent and detect cyber-attacks or ransomware attacks Defendant could and should have implemented, as recommended by the Microsoft Threat Protection Intelligence Team, the following measures:

Secure internet-facing assets

- Apply latest security updates
- Use threat and vulnerability management
- Perform regular audit; remove privileged credentials;

Thoroughly investigate and remediate alerts

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

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

Include IT Pros in security discussions

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

Build credential hygiene

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

Apply principle of least-privilege

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

Harden infrastructure

- Use Windows Defender Firewall
- Enable tamper protection
- Enable cloud-delivered protection
- Turn on attack surface reduction rules and [Antimalware Scan Interface] for Office[Visual Basic for Applications].[6]

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

46. 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 hundreds of

[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/ (last visited Nov. 11, 2021).

thousands of customers,[7] including that of Plaintiff and Class Members.

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

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

48. As a condition of obtaining services at PostMeds, Defendant requires that its customers entrust it with highly sensitive personal information.

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

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

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

52. Upon information and belief, Defendant made promises to Plaintiff and Class Members to maintain and protect their Private Information, demonstrating an understanding of the importance of securing Private Information.

53. 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

[7] https://www.jdsupra.com/legalnews/postmeds-announces-data-breach-6696991/ (last accessed Nov. 3, 2023).

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]

54. Plaintiff 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

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

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

57. 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]

58. In light of recent high profile cybersecurity incidents at healthcare companies that store Private Information, including American Medical Collection Agency (25 million patients, March 2019), University of Washington Medicine (974,000 patients, December 2018), Florida Orthopedic Institute (640,000 patients, July 2020), Wolverine Solutions Group (600,000 patients, September 2018), Oregon Department of Human Services (645,000 patients, March 2019), Elite Emergency Physicians (550,000 patients, June 2020), Magellan Health (365,000 patients, April 2020), and BJC Health System (286,876 patients, March 2020), Defendant knew or should have

[8] https://www.truepill.com/legal/nopp (last accessed Nov. 3, 2023).
[9] *See* https://www.idtheftcenter.org/publication/q3-data-breach-2023-analysis/ (last accessed Oct. 11, 2023).

known that its electronic records would be targeted by cybercriminals.

59. 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]

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

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

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

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

[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 (last accessed Oct. 17, 2022).

Information of Plaintiff and Class Members.

64. The ramifications of Defendant's failure to keep secure the Private Information of Plaintiff 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.

65. As a pharmaceutical company in custody of its current and former customers' Private Information, Defendant knew, or should have known, the importance of safeguarding Private Information entrusted to them by Plaintiff and Class Members, and of the foreseeable consequences if its data security systems were breached. This includes the significant costs imposed on Plaintiff 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

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

67. 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]

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

[11] 17 C.F.R. § 248.201 (2013).
[12] *Id.*

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

70. 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]

71. 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.

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

73. 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."[17]

74. 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

---

[13] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends, Oct. 16, 2019, *available at*: https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last visited Oct. 17, 2022).

[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/ (last visited Oct. 17, 2022).

[15] *In the Dark*, VPNOverview, 2019, *available at*: https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last visited Oct. 217, 2022).

[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/ (last visited May 7, 2023).

[17] https://efraudprevention.net/home/education/?a=187#:~:text=A%20thief%20may%20use%20your,credit%20report%20may%20be%20affected. (last visited Nov. 6, 2023).

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.

75. Between 2005 and 2019, at least 249 million people were affected by healthcare data breaches.[18] Indeed, during 2019 alone, over 41 million healthcare records were exposed, stolen, or unlawfully disclosed in 505 data breaches.[19] 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.[20]

76. According to account monitoring company LogDog, medical data sells for $50 and up on the Dark Web.[21]

77. "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."[22]

78. 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-

---

[18] https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7349636/#B5-healthcare-08-00133/ (last accessed July 24, 2023).

[19] https://www.hipaajournal.com/december-2019-healthcare-data-breach-report/ (last accessed July 24, 2023).

[20] https://www.tenable.com/blog/healthcare-security-ransomware-plays-a-prominent-role-incovid-19-era-breaches/ (last accessed July 24, 2023).

[21] 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 (last accessed July 20, 2021)

[22] Michael Ollove, "The Rise of Medical Identity Theft in Healthcare," Kaiser Health News, Feb. 7, 2014, https://khn.org/news/rise-of-indentity-theft/ (last accessed July 24, 2023).

pocket costs for healthcare they did not receive to restore coverage.[23] 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.[24]

79. 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.

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

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[25]

81. This data, as one would expect, demands a much higher price on the black market. 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."[26]

---

[23] *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/ (last accessed July 24, 2023).

[24] *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/ (last accessed July 24, 2023).

[25] *Report to Congressional Requesters*, GAO, at 29 (June 2007), *available at:* https://www.gao.gov/assets/gao-07-737.pdf (last visited Oct. 17, 2022).

[26] 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 (last visited May 7, 2023).

82. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach because, there, victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change—names, demographic information, and PHI.

Defendant Fails To Comply With FTC Guidelines

83. 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.

84. 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.[27]

85. 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.[28]

86. The FTC further recommends that companies not maintain Private Information

[27] *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 (last visited Oct. 17, 2022).
[28] *Id.*

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.

87. 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.

88. These FTC enforcement actions include actions against pharmaceutical companies, like Defendant.

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

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

91. 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.

Defendant Fails to Comply with HIPAA Guidelines

92. 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.

93. Defendant is subject to the rules and regulations for safeguarding electronic forms of medical information pursuant to the Health Information Technology Act ("HITECH").[29] *See* 42 U.S.C. §17921, 45 C.F.R. § 160.103.

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

95. 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.

96. 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.

97. "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.

98. 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;

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

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

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

d. Ensure compliance by its workforce.

99. 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).

100. 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.

101. 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***."[30]

102. 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).

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

103. 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).

104. 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.[31] 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.[32]

Defendant Fails To Comply With Industry Standards

105. 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.

106. Several best practices have been identified that, at a minimum, should be implemented by pharmaceutical companies in possession of Private Information, like Defendant,

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

including but not limited to: educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data and limiting which employees can access sensitive data. Defendant failed to follow these industry best practices, including a failure to implement multi-factor authentication.

107. 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.

108. 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.

109. 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

110. Defendant breached its obligations to Plaintiff 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 workforces 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.

111. Defendant negligently and unlawfully failed to safeguard Plaintiff's 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.

112. 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 Plaintiff's and Class Members' confidential Private Information.

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

COMMON INJURIES & DAMAGES

114. 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 Plaintiff and Class Members has materialized and is imminent, and Plaintiff 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

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

116. As Plaintiff has 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 Plaintiff and Class Members. Unauthorized individuals can easily access the Private Information of Plaintiff and Class Members.

117. 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.

118. 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.

119. 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.

120. One such example of criminals piecing together bits and pieces of compromised Private Information for profit is the development of "Fullz" packages.[33]

121. 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 in order to assemble complete dossiers on individuals.

122. 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 Plaintiff' and Class Members' phone numbers, email addresses, and other unregulated sources and identifiers. In

[33] "Fullz" is fraudster speak for data that includes the information of the victim, including, but not limited to, the name, address, credit card information, social security number, date of birth, and more. As a rule of thumb, the more information you have on a victim, the more money that can be made off of those credentials. Fullz are usually pricier than standard credit card credentials, commanding up to $100 per record (or more) on the dark web. Fullz can be cashed out (turning credentials into money) in various ways, including performing bank transactions over the phone with the required authentication details in-hand. Even "dead Fullz," which are Fullz credentials associated with credit cards that are no longer valid, can still be used for numerous purposes, including tax refund scams, ordering credit cards on behalf of the victim, or opening a "mule account" (an account that will accept a fraudulent money transfer from a compromised account) without the victim's knowledge. *See*, *e.g.*, Brian Krebs, *Medical Records for Sale in Underground Stolen From Texas Life Insurance Firm*, Krebs on Security (Sep. 18, 2014), https://krebsonsecuritv.eom/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-](https://krebsonsecuritv.eom/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-finn/ (last visited on May 26, 2023).

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.

123. 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 Plaintiff and the other Class Members.

124. 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.

125. 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

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

127. Thus, due to the actual and imminent risk of identity theft, Defendant's Notice Letter encourages Plaintiff 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."[34]

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

129. Plaintiff 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.

130. Plaintiff's 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."[35]

131. Plaintiff's mitigation efforts are also consistent with the steps that FTC recommends that data breach victims take several steps to protect their personal and financial information after a data breach, including: contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for seven years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[36]

Diminution Value Of Private Information

---

[34] Notice Letter.

[35] *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.

[36] *See* Federal Trade Commission, *Identity Theft.gov*, https://www.identitytheft.gov/Steps (last visited July 7, 2022).

132. PII and PHI are valuable property rights.[37] 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.

133. An active and robust legitimate marketplace for PII exists. In 2019, the data brokering industry was worth roughly $200 billion.[38]

134. 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.[39,40]

135. Consumers who agree to provide their web browsing history to the Nielsen Corporation can receive up to $50.00 a year.[41]

136. Conversely sensitive PII can sell for as much as $363 per record on the dark web according to the Infosec Institute.[42]

137. According to account monitoring company LogDog, medical data sells for $50 and up on the Dark Web.[43]

---

[37] *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).

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

[39] https://datacoup.com/

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

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

[42] *See* Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, InfoSec (July 27, 2015), https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/ (last visited Sep. 13, 2022).

[43] 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 (last accessed July 20, 2021)

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

139. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach because, there, victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change, e.g., names, demographic information, and PHI.

140. 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.

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

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

143. 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.

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

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

145. 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 Plaintiff's 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.

146. 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.

147. Furthermore, the information accessed and disseminated in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach, where victims can easily cancel or close credit and debit card accounts.[44] The information

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

disclosed in this Data Breach is impossible to "close" and difficult, if not impossible, to change (such as PHI).

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

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

Loss Of The Benefit Of The Bargain

150. Furthermore, Defendant's poor data security deprived Plaintiff and Class Members of the benefit of their bargain. When agreeing to obtain services from Defendant under certain terms, Plaintiff 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, Plaintiff 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.

PLAINTIFF REED'S EXPERIENCE

151. Plaintiff Richard Reed is a current PostMeds customer.

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

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

154. Plaintiff Richard 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 would not have entrusted his Private Information to Defendant had he known of Defendant's lax data security policies.

155. Plaintiff Richard 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.

156. By deceptively storing, collecting, and disclosing Plaintiff's personal information, Plaintiff overpaid Defendant for services that did not include proper data security for his Private Information.

157. Plaintiff would not have provided his Private Information to Defendant or paid Defendant money for services if Plaintiff had known that Defendant's data security measures were inadequate to protect his Private Information.

158. As a result of the Data Breach, and at the direction of Defendant's Notice Letter, Plaintiff made reasonable efforts to mitigate the impact of the Data Breach, including researching and verifying the legitimacy of the Data Breach upon receiving the Notice Letter, changing passwords and resecuring his own computer network, and contacting companies regarding suspicious activity on his accounts. 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.

159. Plaintiff suffered actual injury from having his Private Information compromised as a result of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) theft of

his 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 his 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.

160. Plaintiff 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.

161. Plaintiff 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.

162. Plaintiff 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.

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

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

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

166. Plaintiff Richard 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.

CLASS ACTION ALLEGATIONS

167. This action is properly maintainable as a class action. Plaintiff brings this class action on behalf of himself and on behalf of all others similarly situated.

168. Plaintiff proposes 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 (the "Class").

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

170. 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 Plaintiff 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).

171. 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 Plaintiff and Class Members;

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

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

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

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

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

g.. Whether Defendant violated the law by failing to promptly notify Plaintiff 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 Plaintiff 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 Plaintiff and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach.

172. Typicality: Plaintiff's claims are typical of those of the other members of the Class because Plaintiff, like every other Class Member, was exposed to virtually identical conduct and now suffers from the same violations of the law as each other member of the Class.

173. 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 Plaintiff's challenge of these policies hinges on Defendant's conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiff.

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

175. Superiority and Manageability: The class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will

permit a large number of Class Members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain Class Members, who could not individually afford to litigate a complex claim against large corporations, like Defendant. Further, even for those Class Members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

176. The nature of this action and the nature of laws available to Plaintiff and Class Members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiff and Class Members for the wrongs alleged because Defendant would necessarily gain an unconscionable advantage since 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 Plaintiff was exposed is representative of that experienced by the Class and will establish the right of each Class Member to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

177. 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.

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

179. 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.

180. 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 under Code of Civil Procedure § 382.

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

181. Plaintiff restates and realleges the preceding factual allegations set forth above as if fully alleged herein.

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

183. Plaintiff and the Class Members entrusted their Private Information to Defendant with the understanding that Defendant would safeguard their information and delete it once the employment relationship terminated.

184. By assuming the responsibility to collect and store this data, and in fact doing so, and sharing it and using it for commercial gain, Defendant had a duty of care to use reasonable means to secure and safeguard their computer property—and Class Members' Private Information held within it—to prevent disclosure of the information, and to safeguard the 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.

185. 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.

186. 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.

187. 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.

188. 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.

189. 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 Plaintiff and the Class.

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

191. 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.

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

193. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and the Class.

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

195. 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.

196. Defendant has full knowledge of the sensitivity of the Private Information and the

types of harm that Plaintiff and the Class could and would suffer if the Private Information were wrongfully disclosed.

197. Plaintiff and the Class were the foreseeable and probable victims of any inadequate security practices and procedures. Defendant knew or should have known of the inherent risks in collecting and storing the Private Information of Plaintiff 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.

198. 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.

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

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

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

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

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

204. There is a close causal connection between Defendant's failure to implement security measures to protect the Private Information of Plaintiff and the Class and the harm, or risk of imminent harm, suffered by Plaintiff and the Class. The Private Information of Plaintiff 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.

205. As a direct and proximate result of Defendant's negligence, Plaintiff and the Class have suffered and will suffer injury, including but not limited to: (i) invasion of privacy; (ii) 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) Plaintiff experiencing suspicious activity on his Venmo account; (viii) Plaintiff's Private Information being disseminated on the dark web, according to CreditWise and Experian; (ix) experiencing an increase in spam calls, texts, and/or emails; (x) statutory damages; (xi) nominal damages; and (xii) 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.

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

207. Additionally, as a direct and proximate result of Defendant's negligence, Plaintiff and the Class have suffered and will suffer the continued risks of exposure of their 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.

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

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

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

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

211. Plaintiff restates and realleges the preceding factual allegations set forth above as if fully alleged herein.

212. Plaintiff and Class Members were required to provide their Private Information to Defendant as a condition of obtaining services at Defendant.

213. Plaintiff 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 Plaintiff and Class Members that it would only disclose Private Information under certain circumstances, none of which relate to the Data Breach.

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

215. Implicit in the agreement between Plaintiff 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 Plaintiff 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 Plaintiff and Class Members from unauthorized disclosure or uses, (f) retain the Private Information only under conditions that kept such information secure and confidential.

216. When Plaintiff 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.

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

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

219. Plaintiff 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.

220. Plaintiff 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.

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

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

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

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

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

226. Plaintiff 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 Plaintiff and the Class)

227. Plaintiff restates and realleges the preceding factual allegations set forth above as

if fully alleged herein.

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

229. Plaintiff 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.

230. Plaintiff 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, Plaintiff and Class Members should have received adequate protection and data security for such Private Information held by Defendant.

231. Defendant benefited from receiving Plaintiff's and Class Members' labor 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.

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

233. Because all Private Information provided by Plaintiff 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.

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

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

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

237. 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 Plaintiff and Class Members by utilizing cheaper, ineffective security measures. Plaintiff and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's failure to provide the requisite security.

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

239. Defendant's enrichment at the expense of Plaintiff and Class Members is and was unjust.

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

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

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

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

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

245. Plaintiff re-alleges and incorporates by reference each and every allegation in this Complaint, as if fully set forth herein.

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

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

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

a. Defendant failed to implement and maintain reasonable security measures to protect Plaintiff's 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 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.

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

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

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's 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 Plaintiff's and Class Members' personal information, including duties imposed by 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 Plaintiff's 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 Plaintiff's and Class Members' personal information, including duties imposed by the FTC Act, 15 U.S.C. § 45 and HIPAA;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff's 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 Plaintiff's and Class Members' personal information, including duties imposed by the FTC Act, 15 U.S.C. § 45.

251. 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.

252. As a direct and proximate result of Defendant's unfair, unlawful, and fraudulent acts and practices, Plaintiff 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.

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

254. Plaintiff 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.

255. By deceptively storing, collecting, and disclosing their personal information, Defendant has taken money or property from Plaintiff and Class Members.

256. By deceptively storing, collecting, and disclosing their personal information,

Plaintiff and Class Members overpaid Defendant for services that did not include proper data security for their Private Information.

257. Plaintiff and Class Members would not have provided their Private Information to Defendant or paid Defendant money for services if Plaintiff and Class Members had known that Defendant's data security measures were inadequate to protect their Private Information.

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

259. Plaintiff 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.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff prays for judgment as follows:

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

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

C. For equitable relief compelling Defendant to utilize appropriate methods and policies with respect to consumer data collection, storage, and safety, and to

disclose with specificity the type of Private Information compromised during the Data Breach;

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

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

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

iii. Requiring Defendant to delete, destroy, and purge the Private Information of Plaintiff and Class Members unless Defendant can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and Class Members;

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

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

vi. Requiring Defendant to engage independent third-party security auditors/penetration testers as well as internal security personnel to

conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

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

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

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

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

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

xii. Requiring Defendant to routinely and continually conduct internal training and education, and on an annual basis to inform internal security

personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

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

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

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

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

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

and to report any deficiencies with compliance of the Court's final judgment.

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

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

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

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

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

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

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

JURY TRIAL DEMANDED

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

Dated: November 6, 2023

Respectfully submitted,

s/ John J. Nelson

John J. Nelson (SBN 317598)
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, LLC
402 W. Broadway, Suite 1760
San Diego, CA 92101
Telephone: (858) 209-6941
Email: jnelson@milberg.com

Attorney for Plaintiff and the Proposed Class

ClassAction.org
