

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.

1           2. Defendant is a digital pharmacy that “operates a nationwide network of URAC-  
2 accredited mail order and specialty pharmacies.”<sup>1</sup>

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

6           4. PostMeds collected and maintained certain personally identifiable information and  
7 protected health information of Plaintiff and the putative Class Members (defined below), who are  
8 (or were) customers at PostMeds.

9           5. The information compromised in the Data Breach included Plaintiff’s and Class  
10 Members’ full names, demographic information (“personally identifiable information” or “PII”)  
11 and medical and health insurance information, which is protected health information (“PHI”, and  
12 collectively with PII, “Private Information”) as defined by the Health Insurance Portability and  
13 Accountability Act of 1996 (“HIPAA”).

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

17           7. As a result of the Data Breach, Plaintiff and Class Members, suffered concrete  
18 injuries in fact including, but not limited to: (i) invasion of privacy; (ii) theft of their Private  
19 Information; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity  
20 costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss  
21 of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the  
22 actual consequences of the Data Breach; (vii) Plaintiff experiencing suspicious activity on his  
23  
24  
25  
26

27 <sup>1</sup> <https://www.truepill.com/> (last accessed Nov. 3, 2023).  
28

1 Venmo account; (viii) Plaintiff's Private Information being disseminated on the dark web,  
2 according to CreditWise and Experian; (ix) experiencing an increase in spam calls, texts, and/or  
3 emails; (x) statutory damages; (xi) nominal damages; and (xii) the continued and certainly  
4 increased risk to their Private Information, which: (a) remains unencrypted and available for  
5 unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's  
6 possession and is subject to further unauthorized disclosures so long as Defendant fails to  
7 undertake appropriate and adequate measures to protect the Private Information.  
8

9 8. The Data Breach was a direct result of Defendant's failure to implement adequate  
10 and reasonable cyber-security procedures and protocols necessary to protect its customers'  
11 Private Information from a foreseeable and preventable cyber-attack.  
12

13 9. Defendant maintained the Private Information in a reckless manner. In particular,  
14 the Private Information was maintained on Defendant's computer network in a condition  
15 vulnerable to cyberattacks. Upon information and belief, the mechanism of the cyberattack and  
16 potential for improper disclosure of Plaintiff's and Class Members' Private Information was a  
17 known risk to Defendant, and thus, Defendant was on notice that failing to take steps necessary  
18 to secure the Private Information from those risks left that property in a dangerous condition.  
19

20 10. Defendant disregarded the rights of Plaintiff and Class Members by, *inter alia*,  
21 intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable  
22 measures to ensure its data systems were protected against unauthorized intrusions; failing to  
23 disclose that they did not have adequately robust computer systems and security practices to  
24 safeguard Class Members' Private Information; failing to take standard and reasonably available  
25 steps to prevent the Data Breach; and failing to provide Plaintiff and Class Members prompt and  
26 accurate notice of the Data Breach.  
27  
28

1           11. Plaintiff's and Class Members' identities are now at risk because of Defendant's  
2 negligent conduct because the Private Information that Defendant collected and maintained is  
3 now in the hands of data thieves.

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

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

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

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

22           16. Through this Complaint, Plaintiff seeks to remedy these harms on behalf of  
23 himself and all similarly situated individuals whose Private Information was accessed during the  
24

1 Data Breach.

2 17. Plaintiff seeks remedies including, but not limited to, compensatory damages and  
3 injunctive relief including improvements to Defendant's data security systems, future annual  
4 audits, and adequate credit monitoring services funded by Defendant.  
5

### 6 **PARTIES**

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

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

### 11 **JURISDICTION AND VENUE**

12 20. This Court has subject matter jurisdiction over this action under 28 U.S.C. § 1332(d)  
13 because this is a class action wherein the amount in controversy exceeds the sum or value of  
14 \$5,000,000, exclusive of interest and costs, there are more than 100 members in the proposed class,  
15 and at least one member of the class, including Plaintiff, is a citizen of a state different from  
16 Defendant.  
17

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

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

### 24 **FACTUAL ALLEGATIONS**

#### 25 ***Defendant's Business***

26  
27  
28

23. Defendant is a digital pharmacy that “operates a nationwide network of URAC-accredited mail order and specialty pharmacies.”<sup>2</sup>

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.<sup>3</sup>

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

---

<sup>2</sup> <https://www.truepill.com/> (last accessed Nov. 3, 2023).

<sup>3</sup> <https://www.truepill.com/legal/nopp> (last accessed Nov. 3, 2023).

1 confidentiality of their Private Information. Plaintiff and Class Members relied on the  
2 sophistication of Defendant to keep their Private Information confidential and securely  
3 maintained, to use this information for necessary purposes only, and to make only authorized  
4 disclosures of this information. Plaintiff and Class Members value the confidentiality of their  
5 Private Information and demand security to safeguard their Private Information.  
6

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

10 32. Defendant had obligations created by FTC Act, HIPAA, contract, industry  
11 standards, and representations made to Plaintiff and Class Members, to keep their Private  
12 Information confidential and to protect it from unauthorized access and disclosure.  
13

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

17 34. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class  
18 Members' Private Information, Defendant assumed legal and equitable duties and knew or should  
19 have known that it was responsible for protecting Plaintiff's and Class Members' Private  
20 Information from disclosure.  
21

### 22 ***The Data Breach***

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

25 **What Happened:** On August 31, 2023, we discovered that a bad actor gained access to  
26 a subset of files used for pharmacy management and fulfillment services. We immediately  
27 launched an investigation with assistance from cybersecurity professionals and worked  
28 quickly to secure our environment.

1           **What Information Was Involved:** Our investigation determined that the bad actor  
2           accessed the files between August 30, 2023 and September 1, 2023. One or more of those  
3           files contained your name and prescription information. The information varied by  
4           individual, but may have included medication type, demographic information, and/or  
          prescribing physician.<sup>4</sup>

5           36.     Omitted from the Notice Letter were any details about what demographic  
6           information was compromised, the details of the root cause of the Data Breach, the vulnerabilities  
7           exploited, and the remedial measures undertaken to ensure such a breach does not occur again.  
8           To date, these critical facts have not been explained or clarified to Plaintiff and Class Members,  
9           who retain a vested interest in ensuring that their Private Information remains protected.  
10          

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

15          38.     Defendant did not use reasonable security procedures and practices appropriate to  
16          the nature of the sensitive information they were maintaining for Plaintiff and Class Members,  
17          causing the exposure of Private Information, such as encrypting the information or deleting it  
18          when it is no longer needed.  
19          

20          39.     The attacker accessed and acquired files Defendant shared with a third party  
21          containing unencrypted Private Information of Plaintiff and Class Members, including their PHI  
22          and other sensitive information. Plaintiff’s and Class Members’ Private Information was accessed  
23          and stolen in the Data Breach.  
24          

25          40.     Plaintiff has already been informed that his Private Information has been  
26          disseminated on the dark web, and Plaintiff further believes that the Private Information of Class  
27          

---

28          <sup>4</sup> 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.<sup>5</sup>

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**

---

<sup>5</sup> *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].<sup>6</sup>

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

---

<sup>6</sup> 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).

1 thousands of customers,<sup>7</sup> including that of Plaintiff and Class Members.

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

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

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

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

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

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

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

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

- 20
- 21 • We are required by law to maintain the privacy and security of your protected
  - 22 health information.
  - 23 • We will let you know promptly if a breach occurs that may have compromised the
  - 24 privacy or security of your information.
  - 25 • We must follow the duties and privacy practices described in this notice and give
- 26

27 <sup>7</sup> <https://www.jdsupra.com/legalnews/postmeds-announces-data-breach-6696991/> (last accessed  
28 Nov. 3, 2023).

1           you a copy of it.

- 2           • We will not use or share your information other than as described here unless you
- 3           tell us we can in writing. If you tell us we can, you may change your mind at any
- 4           time. Let us know in writing if you change your mind.<sup>8</sup>

5           54. Plaintiff and the Class Members relied on Defendant to keep their Private

6 Information confidential and securely maintained, to use this information for business purposes

7 only, and to make only authorized disclosures of this information.

8           ***Defendant Knew or Should Have Known of the Risk Because Pharmaceutical***

9           ***Companies In Possession Of Private Information Are Particularly Susceptable To***

10           ***Cyber Attacks***

11           55. Defendant's data security obligations were particularly important given the

12 substantial increase in cyber-attacks and/or data breaches targeting pharmaceutical companies

13 that collect and store Private Information, like Defendant, preceding the date of the breach.

14           56. Data breaches, including those perpetrated against pharmaceutical companies that

15 store Private Information in their systems, have become widespread.

16           57. In the third quarter of the 2023 fiscal year alone, 7333 organizations experienced

17 data breaches, resulting in 66,658,764 individuals' personal information being compromised.<sup>9</sup>

18           58. In light of recent high profile cybersecurity incidents at healthcare companies that

19 store Private Information, including American Medical Collection Agency (25 million patients,

20 March 2019), University of Washington Medicine (974,000 patients, December 2018), Florida

21 Orthopedic Institute (640,000 patients, July 2020), Wolverine Solutions Group (600,000 patients,

22 September 2018), Oregon Department of Human Services (645,000 patients, March 2019), Elite

23 Emergency Physicians (550,000 patients, June 2020), Magellan Health (365,000 patients, April

24 2020), and BJC Health System (286,876 patients, March 2020), Defendant knew or should have

25

26 <sup>8</sup> <https://www.truepill.com/legal/nopp> (last accessed Nov. 3, 2023).

27 <sup>9</sup> See <https://www.idtheftcenter.org/publication/q3-data-breach-2023-analysis/> (last accessed Oct.

28 11, 2023).

1 known that its electronic records would be targeted by cybercriminals.

2 59. Indeed, cyber-attacks, such as the one experienced by Defendant, have become so  
3 notorious that the Federal Bureau of Investigation (“FBI”) and U.S. Secret Service have issued a  
4 warning to potential targets so they are aware of, and prepared for, a potential attack. As one  
5 report explained, smaller entities that store Private Information are “attractive to ransomware  
6 criminals...because they often have lesser IT defenses and a high incentive to regain access to  
7 their data quickly.”<sup>10</sup>

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

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

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

21 63. The injuries to Plaintiff and Class Members were directly and proximately caused  
22 by Defendant’s failure to implement or maintain adequate data security measures for the Private  
23

24  
25  
26 <sup>10</sup> [https://www.law360.com/consumerprotection/articles/1220974/fbi-secret-service-warn-of-](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)  
27 [targeted-ransomware?nl\\_pk=3ed44a08-fcc2-4b6c-89f0-](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)  
28 [aa0155a8bb51&utm\\_source=newsletter&utm\\_medium=email&utm\\_campaign=consumerprotect](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)  
[ion \(last accessed Oct. 17, 2022\).](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)

1 Information of Plaintiff and Class Members.

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

6 65. As a pharmaceutical company in custody of its current and former customers'  
7 Private Information, Defendant knew, or should have known, the importance of safeguarding  
8 Private Information entrusted to them by Plaintiff and Class Members, and of the foreseeable  
9 consequences if its data security systems were breached. This includes the significant costs  
10 imposed on Plaintiff and Class Members as a result of a breach. Defendant failed, however, to  
11 take adequate cybersecurity measures to prevent the Data Breach.  
12

13 ***Value Of Personally Identifiable Information***  
14

15 66. The Federal Trade Commission ("FTC") defines identity theft as "a fraud  
16 committed or attempted using the identifying information of another person without authority."<sup>11</sup>

17 67. The FTC describes "identifying information" as "any name or number that may  
18 be used, alone or in conjunction with any other information, to identify a specific person,"  
19 including, among other things, "[n]ame, Social Security number, date of birth, official State or  
20 government issued driver's license or identification number, alien registration number,  
21 government passport number, employer or taxpayer identification number."<sup>12</sup>  
22

23 68. The PII of individuals remains of high value to criminals, as evidenced by the  
24 prices they will pay through the dark web.  
25

26  
27 <sup>11</sup> 17 C.F.R. § 248.201 (2013).

28 <sup>12</sup> *Id.*

69. Numerous sources cite dark web pricing for stolen identity credentials.<sup>13</sup>

70. For example, PII can be sold at a price ranging from \$40 to \$200.<sup>14</sup> Criminals can also purchase access to entire company data breaches from \$900 to \$4,500.<sup>15</sup>

71. PII can sell for as much as \$363 per record according to the Infosec Institute.<sup>16</sup> 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.”<sup>17</sup>

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

<sup>13</sup> *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).

<sup>14</sup> *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).

<sup>15</sup> *In the Dark*, VPNOverview, 2019, available at: <https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/> (last visited Oct. 21, 2022).

<sup>16</sup> 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).

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



1 criminals openly post stolen payment card numbers, Social Security numbers, and other personal  
 2 information on several underground internet websites. Unsurprisingly, the pharmaceutical  
 3 industry is at high risk and is acutely affected by cyberattacks, like the Data Breach here.

4 75. Between 2005 and 2019, at least 249 million people were affected by healthcare  
 5 data breaches.<sup>18</sup> Indeed, during 2019 alone, over 41 million healthcare records were exposed,  
 6 stolen, or unlawfully disclosed in 505 data breaches.<sup>19</sup> In short, these sorts of data breaches are  
 7 increasingly common, especially among healthcare systems, which account for 30.03 percent of  
 8 overall health data breaches, according to cybersecurity firm Tenable.<sup>20</sup>

10 76. According to account monitoring company LogDog, medical data sells for \$50  
 11 and up on the Dark Web.<sup>21</sup>

12 77. “Medical identity theft is a growing and dangerous crime that leaves its victims  
 13 with little to no recourse for recovery,” reported Pam Dixon, executive director of World Privacy  
 14 Forum. “Victims often experience financial repercussions and worse yet, they frequently discover  
 15 erroneous information has been added to their personal medical files due to the thief’s  
 16 activities.”<sup>22</sup>

18 78. A study by Experian found that the average cost of medical identity theft is “about  
 19 \$20,000” per incident and that most victims of medical identity theft were forced to pay out-of-  
 20

21  
 22 <sup>18</sup> <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7349636/#B5-healthcare-08-00133/> (last  
 accessed July 24, 2023).

23 <sup>19</sup> <https://www.hipaajournal.com/december-2019-healthcare-data-breach-report/> (last accessed  
 July 24, 2023).

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

25 <sup>21</sup> Lisa Vaas, *Ransomware Attacks Paralyze, and Sometimes Crush, Hospitals*, Naked Security  
 26 (Oct. 3, 2019), [https://nakedsecurity.sophos.com/2019/10/03/ransomware-attacks-paralyze-and-  
 sometimes-crush-hospitals/#content](https://nakedsecurity.sophos.com/2019/10/03/ransomware-attacks-paralyze-and-sometimes-crush-hospitals/#content) (last accessed July 20, 2021)

27 <sup>22</sup> Michael Ollove, “The Rise of Medical Identity Theft in Healthcare,” Kaiser Health News, Feb.  
 28 7, 2014, <https://khn.org/news/rise-of-indentity-theft/> (last accessed July 24, 2023).

1 pocket costs for healthcare they did not receive to restore coverage.<sup>23</sup> Almost half of medical  
 2 identity theft victims lose their healthcare coverage as a result of the incident, while nearly one-  
 3 third of medical identity theft victims saw their insurance premiums rise, and 40 percent were  
 4 never able to resolve their identity theft at all.<sup>24</sup>

5 79. Among other forms of fraud, identity thieves may obtain driver's licenses,  
 6 government benefits, medical services, and housing or even give false information to police.

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

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

16 81. This data, as one would expect, demands a much higher price on the black market.  
 17 Martin Walter, senior director at cybersecurity firm RedSeal, explained, "[c]ompared to credit  
 18 card information, personally identifiable information . . . [is] worth more than 10x on the black  
 19 market."<sup>26</sup>

21 <sup>23</sup> See Elinor Mills, "Study: Medical Identity Theft is Costly for Victims," CNET (Mar. 3, 2010),  
 22 <https://www.cnet.com/news/study-medical-identity-theft-is-costly-for-victims/> (last accessed July  
 24, 2023).

23 <sup>24</sup> *Id.*; see also *Healthcare Data Breach: What to Know About them and What to Do After One*,  
 24 EXPERIAN, [https://www.experian.com/blogs/ask-experian/healthcare-data-breach-what-](https://www.experian.com/blogs/ask-experian/healthcare-data-breach-what-to-know-about-them-and-what-to-do-after-one/)  
 to-know-about-them-and-what-to-do-after-one/ (last accessed July 24, 2023).

25 <sup>25</sup> *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 <sup>26</sup> Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card*  
 27 *Numbers*, Computer World (Feb. 6, 2015), [http://www.itworld.com/article/2880960/anthem-hack-](http://www.itworld.com/article/2880960/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html)  
 28 personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last visited May 7,  
 2023).

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

6  
7        ***Defendant Fails To Comply With FTC Guidelines***

8        83. The Federal Trade Commission (“FTC”) has promulgated numerous guides for  
9 businesses which highlight the importance of implementing reasonable data security practices.  
10 According to the FTC, the need for data security should be factored into all business decision-  
11 making.

12        84. In 2016, the FTC updated its publication, Protecting Personal Information: A  
13 Guide for Business, which established cyber-security guidelines for businesses. These guidelines  
14 note that businesses should protect the personal customer information that they keep; properly  
15 dispose of personal information that is no longer needed; encrypt information stored on computer  
16 networks; understand their network’s vulnerabilities; and implement policies to correct any  
17 security problems.<sup>27</sup>

18  
19        85. The guidelines also recommend that businesses use an intrusion detection system  
20 to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating  
21 someone is attempting to hack the system; watch for large amounts of data being transmitted  
22 from the system; and have a response plan ready in the event of a breach.<sup>28</sup>

23  
24        86. The FTC further recommends that companies not maintain Private Information

25  
26 <sup>27</sup> *Protecting Personal Information: A Guide for Business*, Federal Trade Commission (2016).  
27 Available at [https://www.ftc.gov/system/files/documents/plain-language/pdf-0136\\_proteting-](https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf)  
28 [personal-information.pdf](https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf) (last visited Oct. 17, 2022).

<sup>28</sup> *Id.*

1 longer than is needed for authorization of a transaction; limit access to sensitive data; require  
2 complex passwords to be used on networks; use industry-tested methods for security; monitor for  
3 suspicious activity on the network; and verify that third-party service providers have  
4 implemented reasonable security measures.

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

12  
13 88. These FTC enforcement actions include actions against pharmaceutical  
14 companies, like Defendant.

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

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

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

22  
23 ***Defendant Fails to Comply with HIPAA Guidelines***

24 92. Defendant is a covered entity under HIPAA (45 C.F.R. § 160.102) and is required  
25 to comply with the HIPAA Privacy Rule and Security Rule, 45 C.F.R. Part 160 and Part 164,  
26 Subparts A and E (“Standards for Privacy of Individually Identifiable Health Information”), and  
27  
28

1 Security Rule (“Security Standards for the Protection of Electronic Protected Health  
2 Information”), 45 C.F.R. Part 160 and Part 164, Subparts A and C.

3 93. Defendant is subject to the rules and regulations for safeguarding electronic forms  
4 of medical information pursuant to the Health Information Technology Act (“HITECH”).<sup>29</sup> See  
5 42 U.S.C. §17921, 45 C.F.R. § 160.103.  
6

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

9 95. HIPAA’s Privacy Rule or *Security Standards for the Protection of Electronic*  
10 *Protected Health Information* establishes a national set of security standards for protecting health  
11 information that is kept or transferred in electronic form.  
12

13 96. HIPAA requires “compl[iance] with the applicable standards, implementation  
14 specifications, and requirements” of HIPAA “with respect to electronic protected health  
15 information.” 45 C.F.R. § 164.302.

16 97. “Electronic protected health information” is “individually identifiable health  
17 information ... that is (i) transmitted by electronic media; maintained in electronic media.” 45  
18 C.F.R. § 160.103.

19 98. HIPAA’s Security Rule requires Defendant to do the following:

- 20 a. Ensure the confidentiality, integrity, and availability of all electronic  
21 protected health information the covered entity or business associate  
22 creates, receives, maintains, or transmits;  
23
- 24 b. Protect against any reasonably anticipated threats or hazards to the security  
25 or integrity of such information;  
26

27 <sup>29</sup> HIPAA and HITECH work in tandem to provide guidelines and rules for maintaining protected  
28 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.*”<sup>30</sup>

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).

---

<sup>30</sup> 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.<sup>31</sup> 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.<sup>32</sup>

***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,

<sup>31</sup> <http://www.hhs.gov/hipaa/for-professionals/security/guidance/index.html>.

<sup>32</sup> <https://www.hhs.gov/hipaa/for-professionals/security/guidance/guidance-risk-analysis/index.html>

1 including but not limited to: educating all employees; strong passwords; multi-layer security,  
2 including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable  
3 without a key; multi-factor authentication; backup data and limiting which employees can access  
4 sensitive data. Defendant failed to follow these industry best practices, including a failure to  
5 implement multi-factor authentication.  
6

7 107. Other best cybersecurity practices that are standard in the pharmaceutical industry  
8 include installing appropriate malware detection software; monitoring and limiting the network  
9 ports; protecting web browsers and email management systems; setting up network systems such  
10 as firewalls, switches and routers; monitoring and protection of physical security systems;  
11 protection against any possible communication system; training staff regarding critical points.  
12 Defendant failed to follow these cybersecurity best practices, including failure to train staff.  
13

14 108. Defendant failed to meet the minimum standards of any of the following  
15 frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation  
16 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,  
17 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  
18 for Internet Security's Critical Security Controls (CIS CSC), which are all established standards  
19 in reasonable cybersecurity readiness.  
20

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

25 ***Defendant's Breach***

26 110. Defendant breached its obligations to Plaintiff and Class Members and/or was  
27  
28



1 otherwise negligent and reckless by conducting the following acts and/or omissions:

- 2 a. Failing to maintain an adequate data security system to reduce the risk of data  
3 breaches and cyber-attacks;
- 4 b. Failing to adequately protect Private Information;
- 5 c. Failing to ensure the confidentiality and integrity of electronic Private Information  
6 it created, received, maintained, and/or transmitted;
- 7 d. Failing to implement technical policies and procedures for electronic information  
8 systems that maintain electronic Private Information to allow access only to those  
9 persons or software programs that have been granted access rights;
- 10 e. Failing to implement policies and procedures to prevent, detect, contain, and correct  
11 security violations;
- 12 f. Failing to implement procedures to review records of information system activity  
13 regularly, such as audit logs, access reports, and security incident tracking reports;
- 14 g. Failing to protect against reasonably anticipated threats or hazards to the security  
15 or integrity of electronic Private Information;
- 16 h. Failing to train all members of their workforces effectively on the policies and  
17 procedures regarding Private Information;
- 18 i. Failing to render the electronic Private Information it maintained unusable,  
19 unreadable, or indecipherable to unauthorized individuals;
- 20 j. Failing to comply with FTC guidelines for cybersecurity, in violation of Section 5  
21 of the FTC Act;
- 22 k. Failing to adhere to HIPAA guidelines and industry standards for cybersecurity as  
23 discussed above; and,  
24  
25  
26  
27  
28

1. 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

1 certainly increased risk to their Private Information, which: (a) remains unencrypted and  
2 available for unauthorized third parties to access and abuse; and (b) remains backed up in  
3 Defendant's possession and is subject to further unauthorized disclosures so long as Defendant  
4 fails to undertake appropriate and adequate measures to protect the Private Information.

5  
6 ***The Data Breach Increases Victims' Risk Of Identity Theft***

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

9 116. As Plaintiff has already experienced, the unencrypted Private Information of Class  
10 Members will end up for sale on the dark web because that is the *modus operandi* of hackers. In  
11 addition, unencrypted Private Information may fall into the hands of companies that will use the  
12 detailed Private Information for targeted marketing without the approval of Plaintiff and Class  
13 Members. Unauthorized individuals can easily access the Private Information of Plaintiff and  
14 Class Members.

15  
16 117. The link between a data breach and the risk of identity theft is simple and well  
17 established. Criminals acquire and steal Private Information to monetize the information.  
18 Criminals monetize the data by selling the stolen information on the black market to other  
19 criminals who then utilize the information to commit a variety of identity theft related crimes  
20 discussed below.

21  
22 118. Because a person's identity is akin to a puzzle with multiple data points, the more  
23 accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take  
24 on the victim's identity--or track the victim to attempt other hacking crimes against the individual  
25 to obtain more data to perfect a crime.

26 119. For example, armed with just a name and date of birth, a data thief can utilize a  
27  
28

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.<sup>33</sup>

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

---

<sup>33</sup> “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://krebsonsecurity.com/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-\]\(https://krebsonsecurity.com/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-finn/](https://krebsonsecurity.com/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-](https://krebsonsecurity.com/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-finn/) (last visited on May 26, 2023).

1 other words, even if certain information such as emails, phone numbers, or credit card numbers  
2 may not be included in the Private Information that was exfiltrated in the Data Breach, criminals  
3 may still easily create a Fullz package and sell it at a higher price to unscrupulous operators and  
4 criminals (such as illegal and scam telemarketers) over and over.

5  
6 123. The existence and prevalence of “Fullz” packages means that the Private  
7 Information stolen from the data breach can easily be linked to the unregulated data (like phone  
8 numbers and emails) of Plaintiff and the other Class Members.

9 124. Thus, even if certain information (such as Social Security numbers) was not stolen  
10 in the data breach, criminals can still easily create a comprehensive “Fullz” package.

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

13  
14 ***Loss Of Time To Mitigate Risk Of Identity Theft And Fraud***

15 126. As a result of the recognized risk of identity theft, when a Data Breach occurs,  
16 and an individual is notified by a company that their Private Information was compromised, as  
17 in this Data Breach, the reasonable person is expected to take steps and spend time to address the  
18 dangerous situation, learn about the breach, and otherwise mitigate the risk of becoming a victim  
19 of identity theft or fraud. Failure to spend time taking steps to review accounts or credit reports  
20 could expose the individual to greater financial harm – yet, the resource and asset of time has  
21 been lost.

22  
23 127. Thus, due to the actual and imminent risk of identity theft, Defendant’s Notice  
24 Letter encourages Plaintiff and Class Members to do the following: “We also encourage you to  
25 regularly review your information for accuracy, as a best practice, including information you  
26  
27  
28

1 receive from your healthcare providers.”<sup>34</sup>

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

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

9 130. Plaintiff’s mitigation efforts are consistent with the U.S. Government  
10 Accountability Office that released a report in 2007 regarding data breaches (“GAO Report”) in  
11 which it noted that victims of identity theft will face “substantial costs and time to repair the  
12 damage to their good name and credit record.”<sup>35</sup>

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

19  
20  
21  
22 ***Diminution Value Of Private Information***

23  
24  
25 <sup>34</sup> Notice Letter.

26 <sup>35</sup> 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>.

27 <sup>36</sup> See Federal Trade Commission, *Identity Theft.gov*, <https://www.identitytheft.gov/Steps> (last  
28 visited July 7, 2022).

132. PII and PHI are valuable property rights.<sup>37</sup> 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.<sup>38</sup>

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.<sup>39,40</sup>

135. Consumers who agree to provide their web browsing history to the Nielsen Corporation can receive up to \$50.00 a year.<sup>41</sup>

136. Conversely sensitive PII can sell for as much as \$363 per record on the dark web according to the Infosec Institute.<sup>42</sup>

137. According to account monitoring company LogDog, medical data sells for \$50 and up on the Dark Web.<sup>43</sup>

<sup>37</sup> 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).

<sup>38</sup> <https://www.latimes.com/business/story/2019-11-05/column-data-brokers>

<sup>39</sup> <https://datacoup.com/>

<sup>40</sup> <https://digi.me/what-is-digime/>

<sup>41</sup> Nielsen Computer & Mobile Panel, Frequently Asked Questions, available at <https://computermobilepanel.nielsen.com/ui/US/en/faqs.html>

<sup>42</sup> 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).

<sup>43</sup> 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)

1        138. As a result of the Data Breach, Plaintiff's and Class Members' Private  
2 Information, which has an inherent market value in both legitimate and dark markets, has been  
3 damaged and diminished by its compromise and unauthorized release. However, this transfer of  
4 value occurred without any consideration paid to Plaintiff or Class Members for their property,  
5 resulting in an economic loss. Moreover, the Private Information is now readily available, and  
6 the rarity of the Data has been lost, thereby causing additional loss of value.  
7

8        139. Based on the foregoing, the information compromised in the Data Breach is  
9 significantly more valuable than the loss of, for example, credit card information in a retailer data  
10 breach because, there, victims can cancel or close credit and debit card accounts. The information  
11 compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to  
12 change, e.g., names, demographic information, and PHI.  
13

14        140. Among other forms of fraud, identity thieves may obtain driver's licenses,  
15 government benefits, medical services, and housing or even give false information to police.

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

18        142. At all relevant times, Defendant knew, or reasonably should have known, of the  
19 importance of safeguarding the Private Information of Plaintiff and Class Members, and of the  
20 foreseeable consequences that would occur if Defendant's data security system was breached,  
21 including, specifically, the significant costs that would be imposed on Plaintiff and Class  
22 Members as a result of a breach.  
23

24        143. Defendant was, or should have been, fully aware of the unique type and the  
25 significant volume of data on Defendant's network, amounting to, upon information and belief,  
26 hundreds of thousands of individuals' detailed personal information and thus, the significant  
27  
28



1 number of individuals who would be harmed by the exposure of the unencrypted data.

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

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

6  
7 145. Given the type of targeted attack in this case and sophisticated criminal activity,  
8 the type of Private Information involved, the volume of data obtained in the Data Breach, and  
9 Plaintiff's Private Information already being disseminated on the dark web (as discussed below),  
10 there is a strong probability that entire batches of stolen information have been placed, or will be  
11 placed, on the black market/dark web for sale and purchase by criminals intending to utilize the  
12 Private Information for identity theft crimes –e.g., opening bank accounts in the victims' names  
13 to make purchases or to launder money; file false tax returns; take out loans or lines of credit; or  
14 file false unemployment claims.

15  
16 146. Such fraud may go undetected until debt collection calls commence months, or  
17 even years, later. An individual may not know that his or her Social Security Number was used  
18 to file for unemployment benefits until law enforcement notifies the individual's employer of the  
19 suspected fraud. Fraudulent tax returns are typically discovered only when an individual's  
20 authentic tax return is rejected.

21  
22 147. Furthermore, the information accessed and disseminated in the Data Breach is  
23 significantly more valuable than the loss of, for example, credit card information in a retailer data  
24 breach, where victims can easily cancel or close credit and debit card accounts.<sup>44</sup> The information

25  
26 <sup>44</sup> See Jesse Damiani, *Your Social Security Number Costs \$4 On The Dark Web, New Report Finds*,  
27 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>.  
28

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

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

5 149. The retail cost of credit monitoring and identity theft monitoring can cost around  
6 \$200 a year per Class Member. This is reasonable and necessary cost to monitor to protect Class  
7 Members from the risk of identity theft that arose from Defendant’s Data Breach.  
8

9 ***Loss Of The Benefit Of The Bargain***

10 150. Furthermore, Defendant’s poor data security deprived Plaintiff and Class  
11 Members of the benefit of their bargain. When agreeing to obtain services from Defendant under  
12 certain terms, Plaintiff and other reasonable customers understood and expected that they were,  
13 in part, paying for services and data security to protect their Private Information, when in fact,  
14 Defendant did not provide the expected data security. Accordingly, Plaintiff and Class Members  
15 received services that were of a lesser value than what they reasonably expected to receive under  
16 the bargains they struck with Defendant.  
17

18 **PLAINTIFF REED’S EXPERIENCE**

19 151. Plaintiff Richard Reed is a current PostMeds customer.

20 152. As a condition of obtaining services at PostMeds, Plaintiff was required to provide  
21 his Private Information to Defendant, including his name, demographic information, and PHI.  
22

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

25 154. Plaintiff Richard Reed is very careful about sharing his sensitive Private  
26 Information. Plaintiff stores any documents containing his Private Information in a safe and  
27  
28

1 secure location. He has never knowingly transmitted unencrypted sensitive Private Information  
2 over the internet or any other unsecured source. Plaintiff would not have entrusted his Private  
3 Information to Defendant had he known of Defendant's lax data security policies.

4 155. Plaintiff Richard Reed received the Notice Letter, by U.S. mail, directly from  
5 Defendant, dated October 30, 2023. According to the Notice Letter, Plaintiff's Private  
6 Information was improperly accessed and obtained by unauthorized third parties, including his  
7 name, prescription information, medication type, demographic information, and/or prescribing  
8 physician.  
9

10 156. By deceptively storing, collecting, and disclosing Plaintiff's personal information,  
11 Plaintiff overpaid Defendant for services that did not include proper data security for his Private  
12 Information.  
13

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

17 158. As a result of the Data Breach, and at the direction of Defendant's Notice Letter,  
18 Plaintiff made reasonable efforts to mitigate the impact of the Data Breach, including researching  
19 and verifying the legitimacy of the Data Breach upon receiving the Notice Letter, changing  
20 passwords and resecuring his own computer network, and contacting companies regarding  
21 suspicious activity on his accounts. Plaintiff has spent significant time dealing with the Data  
22 Breach—valuable time Plaintiff otherwise would have spent on other activities, including but not  
23 limited to work and/or recreation. This time has been lost forever and cannot be recaptured.  
24

25 159. Plaintiff suffered actual injury from having his Private Information compromised  
26 as a result of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) theft of  
27  
28

1 his Private Information; (iii) lost or diminished value of Private Information; (iv) lost time and  
2 opportunity costs associated with attempting to mitigate the actual consequences of the Data  
3 Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting  
4 to mitigate the actual consequences of the Data Breach; (vii) statutory damages; (viii) nominal  
5 damages; and (ix) the continued and certainly increased risk to his Private Information, which:  
6 (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b)  
7 remains backed up in Defendant's possession and is subject to further unauthorized disclosures  
8 so long as Defendant fails to undertake appropriate and adequate measures to protect the Private  
9 Information.  
10

11 160. Plaintiff further suffered actual injury in the form of his Private Information being  
12 disseminated on the dark web, according to CreditWise and Experian, which, upon information  
13 and belief, was caused by the Data Breach.  
14

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

18 162. Plaintiff further suffered actual injury in the form of experiencing an increase in  
19 spam calls, texts, and/or emails, which, upon information and belief, was caused by the Data  
20 Breach.  
21

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

25 164. As a result of the Data Breach, Plaintiff anticipates spending considerable time  
26 and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach.  
27  
28

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

3 166. Plaintiff Richard Reed has a continuing interest in ensuring that his Private  
4 Information, which, upon information and belief, remains backed up in Defendant's possession,  
5 is protected and safeguarded from future breaches.  
6

### 7 **CLASS ACTION ALLEGATIONS**

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

10 168. Plaintiff proposes the following Class definition, subject to amendment as  
11 appropriate:  
12

#### 13 **Nationwide Class**

14 All individuals residing in the United States whose Private Information was compromised  
15 in the data breach announced by Defendant in October 2023 (the "Class").

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

21 170. Numerosity: The members of the Class are so numerous that joinder of all members  
22 is impracticable, if not completely impossible. Although the precise number of persons impacted  
23 in the Data Breach is currently unknown to Plaintiff and exclusively in the possession of  
24 Defendant, upon information and belief, hundreds of thousands of persons were impacted in the  
25 Data Breach. The Class is apparently identifiable within Defendant's records, and Defendant has  
26 already identified these individuals (as evidenced by sending them breach notification letters).  
27  
28

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

- 5           a. Whether and to what extent Defendant had a duty to protect the Private  
6 Information of Plaintiff and Class Members;
- 7           b. Whether Defendant had respective duties not to disclose the Private Information  
8 of Plaintiff and Class Members to unauthorized third parties;
- 9           c. Whether Defendant had respective duties not to use the Private Information of  
10 Plaintiff and Class Members for non-business purposes;
- 11           d. Whether Defendant failed to adequately safeguard the Private Information of  
12 Plaintiff and Class Members;
- 13           e. Whether and when Defendant actually learned of the Data Breach;
- 14           f. Whether Defendant adequately, promptly, and accurately informed Plaintiff and  
15 Class Members that their Private Information had been compromised;
- 16           g.. Whether Defendant violated the law by failing to promptly notify Plaintiff and  
17 Class Members that their Private Information had been compromised;
- 18           h. Whether Defendant failed to implement and maintain reasonable security  
19 procedures and practices appropriate to the nature and scope of the information  
20 compromised in the Data Breach;
- 21           i. Whether Defendant adequately addressed and fixed the vulnerabilities which  
22 permitted the Data Breach to occur;
- 23           j. Whether Plaintiff and Class Members are entitled to actual damages, statutory  
24  
25  
26  
27  
28

1 damages, and/or nominal damages as a result of Defendant's wrongful conduct;  
2 and

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

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

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

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

21 175. Superiority and Manageability: The class litigation is an appropriate method for fair  
22 and efficient adjudication of the claims involved. Class action treatment is superior to all other  
23 available methods for the fair and efficient adjudication of the controversy alleged herein; it will  
24

1 permit a large number of Class Members to prosecute their common claims in a single forum  
2 simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and  
3 expense that hundreds of individual actions would require. Class action treatment will permit the  
4 adjudication of relatively modest claims by certain Class Members, who could not individually  
5 afford to litigate a complex claim against large corporations, like Defendant. Further, even for  
6 those Class Members who could afford to litigate such a claim, it would still be economically  
7 impractical and impose a burden on the courts.  
8

9       176. The nature of this action and the nature of laws available to Plaintiff and Class  
10 Members make the use of the class action device a particularly efficient and appropriate procedure  
11 to afford relief to Plaintiff and Class Members for the wrongs alleged because Defendant would  
12 necessarily gain an unconscionable advantage since they would be able to exploit and overwhelm  
13 the limited resources of each individual Class Member with superior financial and legal resources;  
14 the costs of individual suits could unreasonably consume the amounts that would be recovered;  
15 proof of a common course of conduct to which Plaintiff was exposed is representative of that  
16 experienced by the Class and will establish the right of each Class Member to recover on the cause  
17 of action alleged; and individual actions would create a risk of inconsistent results and would be  
18 unnecessary and duplicative of this litigation.  
19

20       177. The litigation of the claims brought herein is manageable. Defendant's uniform  
21 conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class  
22 Members demonstrates that there would be no significant manageability problems with  
23 prosecuting this lawsuit as a class action.  
24

25       178. Adequate notice can be given to Class Members directly using information  
26 maintained in Defendant's records.  
27  
28



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.

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

5           186. Defendant's duty to use reasonable security measures under HIPAA required  
6 Defendant to "reasonably protect" confidential data from "any intentional or unintentional use or  
7 disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to  
8 protect the privacy of protected health information." 45 C.F.R. § 164.530(c)(1). Some or all of the  
9 healthcare and/or medical information at issue in this case constitutes "protected health  
10 information" within the meaning of HIPAA.

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

14           188. Defendant breached its duties, and thus was negligent, by failing to use reasonable  
15 measures to protect Class Members' Private Information. The specific negligent acts and  
16 omissions committed by Defendant include, but are not limited to, the following:

- 17           a. Failing to adopt, implement, and maintain adequate security measures to safeguard  
18           Class Members' Private Information;
- 19           b. Failing to adequately monitor the security of their networks and systems;
- 20           c. Failing to periodically ensure that their email system had plans in place to maintain  
21           reasonable data security safeguards;
- 22           d. Allowing unauthorized access to Class Members' Private Information; and,
- 23           e. Failing to detect in a timely manner that Class Members' Private Information had  
24
- 25
- 26
- 27
- 28

1           been compromised.

2           189. Defendant violated Section 5 of the FTC Act and HIPAA by failing to use  
3 reasonable measures to protect Private Information and not complying with applicable industry  
4 standards, as described in detail herein. Defendant's conduct was particularly unreasonable given  
5 the nature and amount of Private Information it obtained and stored and the foreseeable  
6 consequences of the immense damages that would result to Plaintiff and the Class.  
7

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

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

12          192. Defendant's violation of Section 5 of the FTC Act and HIPAA constitutes  
13 negligence.  
14

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

18          194. A breach of security, unauthorized access, and resulting injury to Plaintiff and the  
19 Class was reasonably foreseeable, particularly in light of Defendant's inadequate security  
20 practices.  
21

22          195. It was foreseeable that Defendant's failure to use reasonable measures to protect  
23 Class Members' Private Information would result in injury to Class Members. Further, the breach  
24 of security was reasonably foreseeable given the known high frequency of cyberattacks and data  
25 breaches in the pharmaceutical industry.

26          196. Defendant has full knowledge of the sensitivity of the Private Information and the  
27  
28

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

3       197. Plaintiff and the Class were the foreseeable and probable victims of any inadequate  
4 security practices and procedures. Defendant knew or should have known of the inherent risks in  
5 collecting and storing the Private Information of Plaintiff and the Class, the critical importance of  
6 providing adequate security of that Private Information, and the necessity for encrypting Private  
7 Information stored on Defendant's systems.  
8

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

11       199. Plaintiff and the Class had no ability to protect their Private Information that was  
12 in, and possibly remains in, Defendant's possession.  
13

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

16       201. Defendant's duty extended to protecting Plaintiff and the Class from the risk of  
17 foreseeable criminal conduct of third parties, which has been recognized in situations where the  
18 actor's own conduct or misconduct exposes another to the risk or defeats protections put in place  
19 to guard against the risk, or where the parties are in a special relationship. *See* Restatement  
20 (Second) of Torts § 302B. Numerous courts and legislatures have also recognized the existence of  
21 a specific duty to reasonably safeguard personal information.  
22

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

25       203. But for Defendant's wrongful and negligent breach of duties owed to Plaintiff and  
26 the Class, the Private Information of Plaintiff and the Class would not have been compromised.  
27  
28

1       204. There is a close causal connection between Defendant's failure to implement  
2 security measures to protect the Private Information of Plaintiff and the Class and the harm, or risk  
3 of imminent harm, suffered by Plaintiff and the Class. The Private Information of Plaintiff and the  
4 Class was lost and accessed as the proximate result of Defendant's failure to exercise reasonable  
5 care in safeguarding such Private Information by adopting, implementing, and maintaining  
6 appropriate security measures.  
7

8       205. As a direct and proximate result of Defendant's negligence, Plaintiff and the Class  
9 have suffered and will suffer injury, including but not limited to: (i) invasion of privacy; (ii) theft  
10 of their Private Information; (iii) lost or diminished value of Private Information; (iv) lost time  
11 and opportunity costs associated with attempting to mitigate the actual consequences of the Data  
12 Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting  
13 to mitigate the actual consequences of the Data Breach; (vii) Plaintiff experiencing suspicious  
14 activity on his Venmo account; (viii) Plaintiff's Private Information being disseminated on the  
15 dark web, according to CreditWise and Experian; (ix) experiencing an increase in spam calls,  
16 texts, and/or emails; (x) statutory damages; (xi) nominal damages; and (xii) the continued and  
17 certainly increased risk to their Private Information, which: (a) remains unencrypted and  
18 available for unauthorized third parties to access and abuse; and (b) remains backed up in  
19 Defendant's possession and is subject to further unauthorized disclosures so long as Defendant  
20 fails to undertake appropriate and adequate measures to protect the Private Information.  
21  
22

23       206. As a direct and proximate result of Defendant's negligence, Plaintiff and the Class  
24 have suffered and will continue to suffer other forms of injury and/or harm, including, but not  
25 limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic  
26 losses.  
27  
28

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

1 implemented written privacy policies whereby it expressly promised Plaintiff and Class Members  
2 that it would only disclose Private Information under certain circumstances, none of which relate  
3 to the Data Breach.

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

7  
8       215. Implicit in the agreement between Plaintiff and Class Members and the Defendant  
9 to provide Private Information, was the latter's obligation to: (a) use such Private Information for  
10 business purposes only, (b) take reasonable steps to safeguard that Private Information, (c) prevent  
11 unauthorized disclosures of the Private Information, (d) provide Plaintiff and Class Members with  
12 prompt and sufficient notice of any and all unauthorized access and/or theft of their Private  
13 Information, (e) reasonably safeguard and protect the Private Information of Plaintiff and Class  
14 Members from unauthorized disclosure or uses, (f) retain the Private Information only under  
15 conditions that kept such information secure and confidential.

16  
17       216. When Plaintiff and Class Members provided their Private Information to Defendant  
18 as a condition of obtaining services at Defendant, they entered into implied contracts with  
19 Defendant pursuant to which Defendant agreed to reasonably protect such information.

20  
21       217. Defendant required Class Members to provide their Private Information as part of  
22 Defendant's regular business practices. Plaintiff and Class Members accepted Defendant's offers  
23 and provided their Private Information to Defendant.

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

1           219. Plaintiff and Class Members would not have entrusted their Private Information to  
2 Defendant in the absence of the implied contract between them and Defendant to keep their  
3 information reasonably secure.

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

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

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

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

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

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

17           226. Plaintiff and Class Members are also entitled to injunctive relief requiring  
18 Defendant to, *e.g.*, (i) strengthen its data security systems and monitoring procedures; (ii) submit  
19 to future annual audits of those systems and monitoring procedures; and (iii) immediately provide  
20 adequate credit monitoring to The Class.

21  
22  
23  
24                                   **COUNT III**  
25                                   **Unjust Enrichment / Quasi Contract**  
26                                   **(On Behalf of Plaintiff and the Class)**

27           227. Plaintiff restates and realleges the preceding factual allegations set forth above as  
28



1 if fully alleged herein.

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

4       229. Plaintiff and Class Members conferred a monetary benefit upon Defendant by  
5 providing payments to Defendant as well as by providing their valuable Private Information to  
6 Defendant.

7  
8       230. Plaintiff and Class Members provided Defendant their Private Information on the  
9 understanding that Defendant would pay for the administrative costs of reasonable data privacy  
10 and security practices and procedures from the revenue it derived therefrom. In exchange, Plaintiff  
11 and Class Members should have received adequate protection and data security for such Private  
12 Information held by Defendant.

13  
14       231. Defendant benefited from receiving Plaintiff's and Class Members' labor and from  
15 receiving their Private Information through its ability to retain and use that information for its own  
16 benefit. Defendant understood and accepted this benefit.

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

20  
21       233. Because all Private Information provided by Plaintiff and Class Members was  
22 similarly at risk from a foreseeable and targeted data breach, Defendant's obligation to safeguard  
23 the Private Information it collected from its customers was inherent to the relationship.

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

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

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

5           237. Instead of providing a reasonable level of security that would have prevented the  
6 Data Breach, Defendant instead made calculated decisions to avoid its data security obligations at  
7 the expense of Plaintiff and Class Members by utilizing cheaper, ineffective security measures.  
8 Plaintiff and Class Members, on the other hand, suffered as a direct and proximate result of  
9 Defendant's failure to provide the requisite security.  
10

11           238. Under the principles of equity and good conscience, Defendant should not be  
12 permitted to retain money belonging to Plaintiff and Class Members, because Defendant failed to  
13 implement appropriate data management and security measures mandated by industry standards.  
14

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

17           240. Defendant acquired the monetary benefit and Private Information through  
18 inequitable means in that they failed to disclose the inadequate security practices previously  
19 alleged.  
20

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

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

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

26           244. Plaintiff and the Class Members are entitled to restitution and disgorgement of all  
27  
28

1 profits, benefits, and other compensation obtained by Defendant, plus attorneys' fees, costs, and  
2 interest thereon.

3 **COUNT IV**  
4 **Violation of the California Unfair Competition Law,**  
5 **Cal. Bus. & Prof. Code §17200 *et seq.***  
6 **(On Behalf of Plaintiff and the Class)**

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

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

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

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

13 a. Defendant failed to implement and maintain reasonable security measures to  
14 protect Plaintiff's and Class Members' personal information from unauthorized  
15 disclosure, release, data breaches, and theft, which was a direct and proximate cause  
16 of the Defendant Data Breach. Defendant failed to identify foreseeable security  
17 risks, remediate identified security risks, and adequately improve security  
18 following previous cybersecurity incidents and known coding vulnerabilities in the  
19 industry;  
20

21 b. Defendant's failure to implement and maintain reasonable security measures also  
22 was contrary to legislatively-declared public policy that seeks to protect consumers'  
23 data and ensure that entities that are trusted with it use appropriate security  
24 measures. These policies are reflected in laws, including the FTC Act (15 U.S.C. §  
25 45), California's Customer Records Act (Cal. Civ. Code § 1798.80 *et seq.*), and  
26 California's Consumer Privacy Act (Cal. Civ. Code § 1798.150);  
27  
28

- 1 c. Defendant's failure to implement and maintain reasonable security measures also  
2 led to substantial consumer injuries, as described above, that are not outweighed by  
3 any countervailing benefits to consumers or competition. Moreover, because  
4 consumers could not know of Defendant's inadequate security, consumers could  
5 not have reasonably avoided the harms that Defendant caused; and  
6  
7 d. Engaging in unlawful business practices by violating Cal. Civ. Code § 1798.82.

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

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

- 11 a. Failing to implement and maintain reasonable security and privacy measures to  
12 protect Plaintiff's and Class Members' personal information, which was a direct  
13 and proximate cause of the Defendant Data Breach;  
14  
15 b. Failing to identify foreseeable security and privacy risks, remediate identified  
16 security and privacy risks, which was a direct and proximate cause of the Defendant  
17 Data Breach;  
18  
19 c. Failing to comply with common law and statutory duties pertaining to the security  
20 and privacy of Plaintiff's and Class Members' personal information, including  
21 duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate  
22 cause of the Defendant Data Breach;  
23  
24 d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff's  
25 and Class Members' personal information, including by implementing and  
26 maintaining reasonable security measures;  
27  
28 e. Misrepresenting that it would comply with common law and statutory duties

1           pertaining to the security and privacy of Plaintiff's and Class Members' personal  
2           information, including duties imposed by the FTC Act, 15 U.S.C. § 45 and HIPAA;

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

5           g. Omitting, suppressing, and concealing the material fact that it did not comply with  
6           common law and statutory duties pertaining to the security and privacy of  
7           Plaintiff's and Class Members' personal information, including duties imposed by  
8           the FTC Act, 15 U.S.C. § 45.  
9

10           251. Defendant's representations and omissions were material because they were likely  
11           to deceive reasonable consumers about the adequacy of Defendant's data security and ability to  
12           protect the confidentiality of consumers' personal information.  
13

14           252. As a direct and proximate result of Defendant's unfair, unlawful, and fraudulent  
15           acts and practices, Plaintiff and Class Members' were injured and lost money or property, which  
16           would not have occurred but for the unfair and deceptive acts, practices, and omissions alleged  
17           herein, time and expenses related to monitoring their financial accounts for fraudulent activity, an  
18           increased, imminent risk of fraud and identity theft, and loss of value of their personal information.  
19

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

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

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

26           256. By deceptively storing, collecting, and disclosing their personal information,  
27  
28

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

3 257. Plaintiff and Class Members would not have provided their Private Information to  
4 Defendant or paid Defendant money for services if Plaintiff and Class Members had known that  
5 Defendant's data security measures were inadequate to protect their Private Information.  
6

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

9 259. Plaintiff and Class Members seek all monetary and nonmonetary relief allowed by  
10 law, including restitution of all profits stemming from Defendant's unfair, unlawful, and fraudulent  
11 business practices or use of their personal information; declaratory relief; reasonable attorneys'  
12 fees and costs under California Code of Civil Procedure § 1021.5; injunctive relief; and other  
13 appropriate equitable relief, including public injunctive relief.  
14

15 **PRAYER FOR RELIEF**

16 WHEREFORE, Plaintiff prays for judgment as follows:

- 17 A. For an Order certifying this action as a class action and appointing Plaintiff and  
18 his counsel to represent the Class;
- 19 B. For equitable relief enjoining Defendant from engaging in the wrongful conduct  
20 complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and  
21 Class Members' Private Information, and from refusing to issue prompt,  
22 complete and accurate disclosures to Plaintiff and Class Members;
- 23 C. For equitable relief compelling Defendant to utilize appropriate methods and  
24 policies with respect to consumer data collection, storage, and safety, and to  
25  
26  
27  
28

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

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

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

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

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

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

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

22 vi. Requiring Defendant to engage independent third-party security  
23 auditors/penetration testers as well as internal security personnel to  
24  
25  
26  
27  
28

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

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

7  
8 viii. Requiring Defendant to audit, test, and train its security personnel  
9 regarding any new or modified procedures;

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

14  
15 x. Requiring Defendant to conduct regular database scanning and securing  
16 checks;

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

23  
24 xii. Requiring Defendant to routinely and continually conduct internal  
25 training and education, and on an annual basis to inform internal security  
26  
27  
28



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

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

8  
9 xiv. Requiring Defendant to implement, maintain, regularly review, and  
10 revise as necessary a threat management program designed to  
11 appropriately monitor Defendant's information networks for threats, both  
12 internal and external, and assess whether monitoring tools are  
13 appropriately configured, tested, and updated;

14  
15 xv. Requiring Defendant to meaningfully educate all Class Members about  
16 the threats that they face as a result of the loss of their confidential  
17 personal identifying information to third parties, as well as the steps  
18 affected individuals must take to protect themselves; and

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

21  
22 xvii. for a period of 10 years, appointing a qualified and independent third  
23 party assessor to conduct a SOC 2 Type 2 attestation on an annual basis  
24 to evaluate Defendant's compliance with the terms of the Court's final  
25 judgment, to provide such report to the Court and to counsel for the Class,  
26  
27  
28

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*