Ronald A. Marron (175650)
Alexis M. Wood (270200)
Kas L. Gallucci (288709)
LAW OFFICES OF RONALD A. MARRON
651 Arroyo Drive
San Diego, CA 92103
Telephone: (619) 696-9006
Facsimile: (619) 564-6665
ron@consumersadvocates.com
alexis@consumersadvocates.com
kas@consumersadvocates.com

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF CALIFORNIA

CHRISTOPHER WILLIAMS, individually and on behalf of all others similarly situated and the general public,

Plaintiff,

v.

POSTMEDS, INC. d/b/a TRUEPILL,

Defendant.

Case No.

CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

Plaintiff Christopher Williams, individually and on behalf of himself and all others similarly situated and the general public, by and through undersigned counsel, asserts the following against Defendant Postmeds, Inc. d/b/a TruePill (hereinafter, "Postmeds" or "Defendant") based upon personal knowledge, where applicable, information and belief, and the investigation of counsel.

INTRODUCTION

1. Postmeds which operates under the name TruePill, is a business-to-business vendor that fulfills prescription orders for a nationwide network of digital pharmacies.

2. Defendant is a digital pharmacy that "operates a nationwide network of URAC-accredited mail order and specialty pharmacies." *See* https://www.truepill.com/ (last visited November 9, 2023).

3. On August 31, 2023, Postmeds identified a cybersecurity incident that compromised files containing patients' Personally Identifiable Information ("PII") and electronically stored Protected Health Information. ("e-PHI").

4. The information that was breached included patient name, prescription information, medication type, prescribing physician and demographic information.

5. On October 30, 2023, Postmeds filed a notice of data breach with the California Attorney General, and began notifying patients of the incident (the "Data Breach Notice Letter"). Attached hereto as **Exhibit A** is a copy of the sample Data Breach Notice Letter transmitted to its patients.

6. The Data Breach Notice Letter downplayed the severity of the intrusion stating "Importantly, your social security number was not involved as Postmeds does not receive this information." The letter does not offer free access to credit or identify monitoring services and instead encourages the data breach victims to "regularly review [their] information for accuracy, as a best practice, including information [they] receive from [their] healthcare providers."

7. Further, the Data Breach Notice Letter did not contain any information about what demographic information was compromised, the details of the root cause of the data breach, the vulnerabilities exploited, and the remedial measures undertaken to ensure such a breach does not

occur again.

8. Medical information, like the highly sensitive and confidential e-PHI compromised here, is some of the most sensitive forms of personal information, as it is immutable and cannot be changed. Postmeds' egregious handling of this confidential and sensitive e-PHI, which is now in the hands of bad actors, constitutes an extreme invasion of privacy. Patients consistently recognize the importance of protecting medical information. A survey by the *Institute for Health Freedom* found that 78% of patients feel it is "very important" that their medical records be kept confidential. As a result of the data mishandling, Plaintiff and Class members no longer have control over their e-PHI, which was unsecured for one month with access to a multitude of potential bad actors.

9. Given the highly sensitive and confidential nature of the e-PHI compromised in this incident, Plaintiff and Class members will be required to expend significant time and effort to mitigate the effects of this failure by Defendant to safeguard sensitive information, such as monitoring their credit reports and accounts for fraud.

10. This risk is ongoing because, unlike a credit card, there is no way to cancel e-PHI. The U.S. Department of Health and Human Services ("HHS") has identified several imminent risks as a result of hackers obtaining patients' e-PHI including: (1) medical identity theft, i.e., the use of a patients' medical information to obtain medical services, such as medical prescriptions, surgery, or other medical treatment, as well as counterfeit settlements against health insurers; (2) the weaponization of medical data, i.e., the use of medical data to threaten, extort, or influence the patient to extort money or disparage someone; (3) financial fraud, i.e., the use of e-PHI to create credit card or bank accounts in the patients' name, taking out loans or lines of credit in the patients' name, or the filing of fraudulent tax documents or insurance information; and (4) cyber campaigns, using the medical data in combination with other information on the dark web to commit fraud, identity theft, conduct phishing or scams, or obtain the patients' credentials for other services. Any "unauthorized person" who breached Postmeds' system can continue to exploit this information at the expense of Plaintiff and the Class. This ongoing imminent risk can often persist for years, as identity thieves often hold stolen data for long periods of time before using it.

11. Such careless handling of e-PHI is prohibited by federal and state law. For example, the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") requires healthcare providers, and their business associates, like Postmeds, to safeguard patient e-PHI through a multifaceted approach that includes, among other things: (a) ensuring the confidentiality, integrity, and availability of all e-PHI they create, receive, maintain or transmit; (b) proactively identifying and protecting against reasonably anticipated threats to the security or integrity of e-PHI; (c) protecting against reasonably anticipated, impermissible uses or disclosures of e-PHI; (d) putting in place the required administrative, physical and technical safeguards to protect e-PHI; (e) implementing policies and procedures to prevent, detect, contain, and correct security violations; (f) effectively training their workforce regarding the proper handling of e-PHI; and (g) designating individual security and privacy officers to ensure compliance with these policies and procedures.

12. Postmeds' failure to comply with HIPAA and other laws and/or guidelines as alleged herein by, among other things, failing to take reasonable steps to safeguard patients' highly sensitive and confidential e-PHI, has directly resulted in injury to Plaintiff and the Class.

13. Given the secret nature of, among other things: (a) Postmeds' policies, procedures, systems, and controls; (b) the result of the "investigation" into the incident disclosed in the Data Breach Notice Letter; and (c) communications among Postmeds and/or the cybersecurity professionals who conducted the investigation concerning the data breach referenced in the Data Breach Notice Letter, Plaintiff believes that further evidentiary support for their claims will be unearthed after a reasonable opportunity for discovery.

14. Plaintiff and Class members bring claims for invasion of their privacy interests, as established through California's privacy laws and California's Constitution. In addition, Postmeds' actions constitute negligence, breach of implied contract, unjust enrichment, as well as violations of several state consumer protection and privacy laws.

15. Plaintiff seeks to remedy these harms on behalf of himself and all similarly situated individuals whose highly sensitive and confidential e-PHI was stolen in the data breach. Plaintiff and Class members seek remedies including but not limited to statutory damages, compensatory damages, and injunctive relief requiring substantial improvements to Postmeds' security systems.

PARTIES

I. PLAINTIFF

16. Plaintiff Christopher Williams ("Plaintiff Williams"), is a natural person and citizen of the State of California and a resident of Los Angeles County.

17. As a condition to obtaining services at Postmeds, Plaintiff Williams was required to provide his private e-PHI to Defendant.

18. On or about October 31, 2023, Postmeds notified Plaintiff Williams that his highly sensitive and confidential e-PHI was compromised as a result of unauthorized access to Postmeds files.

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

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

21. Given that Plaintiff Williams highly sensitive and confidential e-PHI was accessed and exfiltrated without his consent as a result of the data breach, Plaintiff Williams has suffered concrete harm, including: (1) the unauthorized disclosure of his private health information to third parties; (2) the imminent risk of fraud and identity theft; (3) the intrusion upon seclusion and violation of his reasonable expectation of privacy in such highly sensitive medical information, such as that related to his medical history and treatment; and (4) emotional distress on dealing with the breach.

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

23. As a result of the data breach, Plaintiff Williams is at present risk and will continue to be at an increased risk of identity theft and fraud for years to come.

II. DEFENDANT POSTMEDS

24. Defendant Postmeds is a corporation organized under the laws of Delaware, having a principal place of business at 3121 Diablo Avenue Hayward, California 94545.

25. On August 31, 2023, it is understood that Postmeds first discovered that an unauthorized third party had gained access to certain files used for pharmacy management and prescription fulfillment services. A purported subsequent investigation by Postmeds revealed that the threat actor had perpetrated the attack between August 30 and September 1 of this year (the "Data Breach").

JURISDICTION AND VENUE

26. This Court has jurisdiction over the subject matter of this action pursuant to 28 U.S.C § 1332(d), because there are more than 100 putative members of the Classes, as defined below, a significant portion of putative Class members are citizens of a state different from Defendant, and the amount in controversy for the Classes exceeds $5,000,000 exclusive of interest and costs. Given the estimated size of the class statutory damages available to Plaintiff and Class members under the CMIA far exceed the $5 million threshold. As does the likely value of any injunctive relief, including changes to Postmeds' systems and procedures to prevent future data breaches, and the value of Plaintiff's and Class members' right to seclusion and non-disclosure of their confidential and sensitive e-PHI.

27. This Court has personal jurisdiction over Postmeds because Defendant maintains its principal executive offices in Hayward, California and is a registered California corporation.

28. This Court has personal jurisdiction over Postmeds because Postmeds has sufficient minimum contacts in California. For example, Postmeds purposefully availed itself of the privileges and benefits associated with conducting business in this state, by, among other things, reaching into California to establish an affiliated partnerships with pharmacies located in California.

29. Venue is proper in this District pursuant to 28 U.S.C. §1391(b)(2) because Defendant transacts business in this District and a substantial portion of the events giving rise to the claims occurred in this District.

FACTUAL BACKGROUND

I. POSTMEDS FAILED TO COMPLY WITH HIPAA, THE NATIONAL STANDARD FOR PROTECTING PRIVATE HEALTH INFORMATION

30. HIPAA requires the healthcare industry to have a generally accepted set of security standards for protecting health information. HIPAA defines Protected Health Information ("PHI") as individually identifiable health information and e-PHI that is transmitted by electronic media or maintained in electronic media. This protected information includes: names, dates, phone numbers, fax numbers, email addresses, SSNs, medical record numbers, health insurance beneficiary numbers, account numbers, certificate/license numbers, vehicle identifiers, device identifiers and serial numbers, URLs, IP addresses, biometric identifiers, photographs, and any other unique identifying number, characteristic, or code.

31. To this end, the Health and Human Services ("HHS") promulgated the HIPAA Privacy Rule in 2000 and the HIPAA Security Rule in 2003. The security standards for the protection of e-PHI, known as "the Security Rule," establish a national set of security standards for protecting certain health information that is held or transferred in electronic form. The Security Rule operationalizes the protections contained in the Privacy Rule by addressing the technical and non-technical safeguards that organizations called "covered entities" must put in place to secure individuals' e-PHI.

32. Defendant is either an entity covered by HIPAA, *see* 45 C.F.R. § 160.102, or "business associates" covered by HIPAA, *see* 45 C.F.R. § 160.103, and therefore must comply with the HIPAA Privacy Rule and Security Rule, *see* 45 C.F.R. Part 160 and Part 164, Subparts A, C, and E.

33. HIPAA limits the permissible uses of e-PHI and prohibits the unauthorized disclosure of e-PHI. *See* 45 C.F.R. § 164.502. HIPAA also requires that covered entities implement appropriate safeguards to protect this information. *See* 45 C.F.R. § 164.530(c)(1).

34. The electronically stored healthcare information accessed by unauthorized third parties on Postmeds' servers are e-PHI under the HIPAA Privacy Rule and the Security Rule, which protects all e-PHI a covered entity "creates, receives, maintains or transmits" in electronic form. 45 C.F.R. § 160.103.

35. The Security Rule requires covered entities or their "business associates", including Postmeds, to implement and maintain appropriate administrative, technical, and physical safeguards for protecting e-PHI. *See* 45 C.F.R. § 164.530(c)(1). Among other things, the Security Rule requires scripts to identify and "[p]rotect against any reasonably anticipated threats or hazards to the security or integrity of [the] information" and "[p]rotect against any reasonably anticipated uses or disclosures." 45 C.F.R. § 164.306.

36. HIPAA also obligates Postmeds to implement policies and procedures to prevent, detect, contain, and correct security violations. *See* 45 C.F.R. § 164.308(a)(1)(i).

37. HIPAA further obligates Postmeds to ensure that their workforce comply with HIPAA security standard rules, *see* 45 C.F.R. § 164.306(a)(4), to effectively train their workforces on the policies and procedures with respect to protected health information, as necessary and appropriate for those individuals to carry out their functions and maintain the security of protected health information. *See* 45 C.F.R. § 164.530(b)(1).

38. Postmeds failed to comply with these HIPAA rules. Specifically, Postmeds failed to put in place the necessary technical and non-technical safeguards required to protect Plaintiff's and Class members' highly sensitive and confidential e-PHI.

II. POSTMEDS VIOLATED THE FTC ACT

39. Postmeds was (and still is) prohibited from engaging in "unfair or deceptive acts or practices in or affecting commerce" by the Federal Trade Commission Act, 15 U.S.C. § 45. Their failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data constitutes an unfair act or practice that violates this rule.

40. In 2007, the FTC published guidelines establishing reasonable data security practices for businesses. The guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies for installing vendor-approved patches to correct security problems. The guidelines also recommend that businesses consider using an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone may be

trying to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.

41. The FTC has also published a document entitled "FTC Facts for Business," which highlights the importance of having a data security plan, regularly assessing risks to computer systems, and implementing safeguards to control such risks.

42. Postmeds was aware of and failed to follow the FTC guidelines and failed to adequately secure patients' data stored on their servers. Furthermore, by failing to have reasonable data security measures in place, Defendant engaged in an unfair act or practice within the meaning of § 5 of the FTC Act.

43. In addition to the FTC Act, Postmeds had a duty to adopt reasonable data security measures in accordance with federal law under HIPAA as well as the laws of the various states in which it operates, including the CMIA.

III. POSTMEDS VIOLATED THEIR COMMON LAW DUTY OF REASONABLE CARE

44. In addition to obligations imposed by federal and state law, Postmeds owed and continues to owe a common law duty to Plaintiff and Class members—who entrusted Postmeds with their highly sensitive and confidential e-PHI—to exercise reasonable care in receiving, maintaining, storing, and deleting the e-PHI in Defendant's possession.

45. Postmeds owed and continues to owe a duty to prevent Plaintiff's and Class members' highly sensitive and confidential e-PHI from being compromised, lost, stolen, accessed, or misused by unauthorized third parties. An essential part of Defendant's duty was (and is) the obligation to provide reasonable security consistent with current industry best practices and requirements, and to ensure information technology systems and networks, in addition to the personnel responsible for those systems and networks, adequately protected and continue to protect Plaintiff's and Class members' highly sensitive and confidential e-PHI.

46. Postmeds owed a duty to Plaintiff and Class members, who entrusted the Defendant with their highly sensitive and confidential e-PHI, to design, maintain, and test the information technology systems that housed Plaintiff's and Class members' highly sensitive and confidential

e-PHI, to ensure that the highly sensitive and confidential e-PHI in Defendant's possession was adequately secured and protected.

47. Postmeds owed a duty to Plaintiff and Class members to create, implement, and maintain reasonable data security practices and procedures sufficient to protect the highly sensitive and confidential e-PHI stored in Postmeds' computer systems. This duty required Postmeds to adequately train employees and others with access to Plaintiff's and Class members' highly sensitive and confidential e-PHI on the procedures and practices necessary to safeguard such sensitive information.

48. Postmeds owed a duty to Plaintiff and Class members to implement processes that would enable Postmeds to timely detect a breach of its information technology systems, and a duty to act upon any data security warnings or red flags detected by such systems in a timely fashion.

49. Postmeds owed a duty to Plaintiff and Class members to disclose when and if Postmeds' information technology systems and data security practices were not sufficiently adequate to protect and safeguard Plaintiff's and Class members' highly sensitive and confidential e-PHI.

50. Defendant violated these duties. Postmeds did not implement measures designed to timely detect a breach of their information technology systems, as required to adequately safeguard Plaintiff's and Class members' highly sensitive and confidential e-PHI. Defendant also violated its duty to create, implement, and maintain reasonable data security practices and procedures sufficient to protect Plaintiff's and Class members' highly sensitive and confidential e-PHI. As the Data Breach Notice Letter states, an investigation began immediately ***after*** it was discovered that bad actors gained access to confidential PHI. Postmeds should have taken these steps ***beforehand*** to protect the highly sensitive and confidential e-PHI in their possession and prevent the unauthorized access from occurring, as required under HIPAA and FTC guidelines, as well as other state and federal law and/or regulations.

51. Postmeds owed a duty to Plaintiff and Class members to timely disclose the fact that a data breach, resulting in unauthorized access to their highly sensitive and confidential e-PHI, had occurred.

IV. POSTMEDS FAILED TO COMPLY WITH THEIR OWN PRIVACY POLICY AND OTHER REPRESENTATIONS

52. Postmeds' Privacy Policy lists the ways that Patient Information may be used and shared. It states: "We may use and share your information as we: 1) treat you 2) Run own organization 3) Bill for your services 4) Help with public health and safety issues 5) Comply with the Law 6) Do research 7) Respond to organ tissue and donation requests 8) Work with a medical examiner or funeral director 9) Address workers' compensation, law enforcement, and other government requests 10) Respond to lawsuits and other legal actions.[1]

53. Postmeds' Privacy Policy further states "we are required by law to maintain the privacy and security of your protected health information" and "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." *Id.*

54. Critically, none of the permissible uses in Postmeds' Privacy Policy of e-PHI include granting unfettered access to unauthorized third parties who have the ability to misuse such information for illicit purposes.

55. Furthermore, as to Postmeds security standards, the Defendant states as follows: "Truepill takes the security of information very seriously and has established security standards and procedures to prevent unauthorized access to patient information. We maintain physical, electronic, and procedural safeguards to comply with federal standards to guard health information, including storing all information you provide to us on our secure servers behind firewalls. Any payment transactions will be encrypted using SSL technology".[2]

56. By these representations in the Privacy Policy, Postmeds affirmatively—and misleadingly—assured patients, including Plaintiff and the Class members, that they had the ability to control the dissemination of their highly sensitive and confidential e-PHI and to restrict its use and access by third parties.

---

[1] https://www.truepill.com/legal/nopp (last accessed November 9, 2023).

[2] https://www.truepill.com/legal/privacy (last accessed November 9, 2023).

57. However, Defendant failed to safeguard patients' highly sensitive and confidential e-PHI in violation of their own Privacy Policy and applicable law and regulations, as confirmed by the Data Breach Notice Letter, in which Postmeds admits that patient data was accessible to unauthorized actors between August 30, 2023 and September 1, 2023. Thus, it is clear that Postmeds failed to take the necessary steps to safeguard Plaintiff's and Class members' highly sensitive and confidential e-PHI until after the data breach incident occurred.

58. Postmeds failure to implement appropriate security measures and adequately safeguard Plaintiff's and Class members' highly sensitive and confidential e-PHI violated the terms of their own Privacy Policy and other representations.

V. THE DATA BREACH DAMAGES PLAINTIFF AND CLASS MEMBERS

59. As a result of Postmeds' deficient security measures, Plaintiff and Class members have been harmed by the compromise of their highly sensitive and confidential e-PHI.

60. Several criminal syndicates, including Ukraine's UNC1878 and China's Dynamite Panda, along with various state-sponsored groups, are known to target hospitals and healthcare providers based on the high value associated with e-PHI, both as a revenue stream (e.g., when sold on the dark web, or used to commit identify theft) and as a tool for executing future hacks (e.g., by impersonating users or providing information that can be useful in cracking passwords or security questions). Plaintiff reasonably anticipates that the identity of any and all hackers involved in this security incident will be revealed in discovery.

61. This exfiltrated highly sensitive and confidential e-PHI can be used for malicious purposes, including doxing, harassment, financial fraud, medical identity theft, identity theft, insurance fraud, and crafting convincing phishing messages. Plaintiff and Class members face an imminent risk of:

a. *medical identity theft*—the use of another person's medical information to obtain a medical service;

b. *weaponizing of medical data*—the use of sensitive medical data to threaten, harass, extort, or influence individuals;

c. *financial fraud*—the use of personally identifiable information contained in medical records to create credit card or bank or insurance profiles to

facilitate financial and insurance fraud; and,

d. *cyber campaigns*—the use of medical data as complementary data in future hacking campaigns.

62. As a result, e-PHI has become increasingly valuable on the black market. In fact, it is more valuable than any other type of record on the dark web. For example, according to *Forbes*, as of April 14, 2017, the going rate for an SSN is $.010 cents and a credit card number is worth $.025 cents, but medical records containing e-PHI could be worth hundreds or even thousands of dollars. For example, in April of 2019, HHS estimated that the average price of medical records containing e-PHI ranged between $250 and $1,000.

63. The Fifth Annual Study on Medical Identity Theft conducted by the *Ponemon Institute* concluded that medical identity theft alone costs the average victim $13,500 to fix.

64. According to *The World Privacy Forum*, a nonprofit public interest group, one of the reasons for this price differential is that criminals are able to extract larger illicit profits using medical records than they are for a credit card or SSN. For example, while a credit card or SSN typically yields around $2,000 before being canceled or changed, an individual's e-PHI typically yields $20,000 or more. This is because, in addition to the fact that healthcare data and e-PHI are immutable (e.g., you cannot cancel your medical records), healthcare data breaches often take much longer to be discovered, allowing thieves to leverage e-PHI for an extended period of time.

65. Further, identity thieves can combine data stolen in the data breach with other information about Plaintiff and Class members gathered from underground sources, public sources, or even Plaintiff's and Class members' social media accounts. Thieves can use the combined data to send highly targeted phishing emails to Plaintiff and Class members to obtain more sensitive information, placing Plaintiff and Class members at further risk of harm. Thieves can use the combined data to commit potential crimes, including opening new financial accounts in Plaintiff's and Class members' names, making false insurance claims using Plaintiff's and Class members' insurance information, taking out loans in Plaintiff's and Class members' names, using Plaintiff's and Class members' information to obtain government benefits, filing fraudulent tax

returns using Plaintiff's and Class members' information, obtaining driver's licenses in Plaintiff's and Class members' names but with another person's photograph.

66. Researchers at HealthITSecurity.com have also reported criminals selling illicit access to compromised healthcare systems on the black market, which would give other criminals "access to their own post-exploitation activity, such as obtaining and exfiltrating sensitive information, infecting other devices in the compromised network, or using connections and information in the compromised network to exploit trusted relationships between the targeted organizations and other entities to compromise additional networks."

67. Given the value of e-PHI, health care providers such as Postmeds are prime targets for cyberattacks, like the data breach that occurred here. Indeed, one recent report indicates that the number of healthcare cyberattacks in the United States has increased by 55% between 2020 and 2021 alone.

68. As to the imminent risk of fraud and identity theft, Plaintiff and Class members will be required to spend substantial amounts of time monitoring their accounts for identity theft and fraud, the opening of fraudulent accounts, disputing fraudulent transactions, and reviewing their financial affairs more closely than they otherwise would have done but for the data breach incident. These efforts are burdensome and time-consuming. Many Class members will also incur out-of-pocket costs for protective measures such as identity theft protection, credit monitoring fees, credit report fees, credit freeze fees, fees for replacement cards in the event of fraudulent charges, and similar costs related to the data breach.

69. The risk of identity theft and fraud will persist for years. Identity thieves often hold stolen data for months or years before using it to avoid detection. Also, the sale of stolen information on the dark web may take months or more to reach end-users, in part because the data is often sold in small batches as opposed to in bulk to a single buyer. Thus, Plaintiff and Class members must vigilantly monitor their financial accounts indefinitely.

70. Postmeds acknowledges that Plaintiff and Class members face a significant risk of various types of identity theft stemming from the data breach. Attempting to shift the burden of responding to the data breach to patients, Postmeds recommended to Plaintiff and affected patients

that they "regularly review your information for accuracy, as a best practice, including information you receive from your healthcare providers." Thus, Postmeds acknowledges that Plaintiff and Class members face an actual imminent risk of fraud and identity theft that requires not only immediate action but continuous, ongoing monitoring.

71. Postmeds has not offered any credit or identity theft monitoring to affected patients. Thus, what Defendant is doing is wholly insufficient to combat the indefinite and undeniable risk of identity theft and fraud, amongst other risks, that may continue long after the data breach.

72. Plaintiff and Class members were also harmed because they were promised services that Postmeds represented would include reasonable security measures to protect their highly sensitive and confidential e-PHI but that, in reality, did not. Plaintiff and Class members would have requested to opt out of Postmeds' services and not have agreed to provide their highly sensitive and confidential e-PHI had they known that these representations were false.

73. Lastly, Plaintiff and Class members have been harmed by Postmeds' intrusion upon their seclusion and invasion of their privacy rights. Postmeds configured their systems in such a way to make Plaintiff's and Class members' highly sensitive and confidential e-PHI exfiltrateable and available without their consent. As a result of Defendant's conduct, unauthorized persons had access to Plaintiff's and Class members' highly sensitive and confidential e-PHI, in which Plaintiff and Class members had a reasonable expectation of privacy.

VI. POSTMEDS' USERS HAVE A REASONABLE EXPECTATION OF PRIVACY

74. Plaintiff and Class members have a reasonable expectation of privacy in their intimate health data, which Postmeds collected, stored, and provided unfettered access to unauthorized third parties. This expectation of privacy is deeply enshrined in California's Constitution.

75. Article I, Section 1 of the California Constitution provides: "All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness***, and privacy***." Art. I., Sec. 1, Cal. Const (emphasis added).

76. The phrase "and privacy" was added in 1972 after voters approved a legislative constitutional amendment designated as Proposition 11. Critically, the argument in favor of Proposition 11 reveals that the legislative intent was to curb businesses' control over the unauthorized collection and use of consumers' personal information, stating in relevant part:

> The right of privacy is the right to be left alone . . . It prevents government and business interests from collecting and stockpiling unnecessary information about us and from misusing information gathered for one purpose in order to serve other purposes or to embarrass us.
>
> **Fundamental to our privacy is the ability to control circulation of personal information.** This is essential to social relationships and personal freedom. The proliferation of government and business records over which we have no control limits our ability to control our personal lives. Often we do not know that these records even exist and we are certainly unable to determine who has access to them.[3]

(emphasis added).

77. Consistent with this language, an abundance of studies examining the collection of consumers' personal data confirms that the surreptitious unauthorized disclosure of highly sensitive and confidential e-PHI from hundreds of thousands of individuals, as Postmeds has done here, violates expectations of privacy that have been established as general social norms.

78. Privacy polls and studies uniformly show that the overwhelming majority of Americans consider one of the most important privacy rights to be the need for an individual's affirmative consent before a company collects and shares its customers' personal data.

79. Surveys consistently show that individuals care about the security and privacy of their e-PHI. In 2013, the *Office of the National Coordinator for Health Information Technology* found that 7 out of 10 individuals are concerned about the privacy of their medical records. The same study found that 3 out of 4 individuals are concerned about the security of their medical records.

---

[3] Ballot Pamp., Proposed Amends. to Cal. Const. with arguments to voters, Gen. Elec. (Nov. 7, 1972) at 27.

80. Likewise, a *Gallup* survey found that 78% of adults believe that it is very important that their medical records be kept confidential, and a majority of respondents believe no one should be permitted to see their records without consent.

81. A recent study by *Consumer Reports* shows that 92% of Americans believe that internet companies and websites should be required to obtain consent before sharing their data and the same percentage believe internet companies and websites should be required to provide consumers with a complete list of the data that has been collected about them.

82. Consistent with these expectations, Plaintiff and Class members have taken steps specifically to ensure the confidentiality of their medical and treatment information, including not disclosing this information to others and even obscuring the specific treatment on insurance records.

83. Despite Plaintiff and Class members expectation of privacy, Postmeds has failed to obtain adequate authorization and data security practices in connection with its data collection practices and the unauthorized disclosure that occurred. This constitutes a violation of Plaintiff' and Class members' privacy interests, including those explicitly enshrined in the California Constitution.

CLASS ACTION ALLEGATIONS

NATIONWIDE CLASS

84. Plaintiff brings this case as a class action pursuant to Fed. R. Civ. P. 23(a), 23(b)(2) and (b)(3) on behalf of the following Nationwide Class:

> All persons in the United States whose e-PHI was compromised between August 30, 2023 and September 1, 2023, due to the incident made public by Postmeds on or around October 30, 2023 (the "**Nationwide Class**").

85. Excluded from the Nationwide Class is Defendant and its subsidiaries and affiliates; all employees of Defendant and its subsidiaries and affiliates; all persons who make a timely election to be excluded from the Nationwide Class; Plaintiff's counsel and Defendant's counsel and members of their immediate families; government entities; and the judge to whom this case is assigned, including his/her immediate family and court staff.

86. Plaintiff reserves the right to modify, expand or amend the above Class definitions or to seek certification of a class or classes defined differently than above before any court determines whether certification is appropriate following discovery.

CALIFORNIA SUBCLASS

87. Plaintiff bring this case as a class action pursuant to Fed. R. Civ. P. 23(a), 23(b)(2) and (b)(3) on behalf of the following California Subclass:

> All persons in the State of California whose e-PHI was compromised between August 30, 2023 and September 1, 2023, due to the incident made public by Postmeds on October 30, 2023, by filing a notice with the California Attorney General (the "**California Subclass**").

88. Excluded from the California Subclass is Defendant and its subsidiaries and affiliates; all employees of Defendant and its subsidiaries and affiliates; all persons who make a timely election to be excluded from the California Class; Plaintiff's counsel and Defendant's counsel and members of their immediate families; government entities; and the judge to whom this case is assigned, including his/her immediate family and court staff.

89. Plaintiff reserves the right to modify, expand or amend the above Subclass definitions or to seek certification of a class or classes defined differently than above before any court determines whether certification is appropriate following discovery.

90. Certification of Plaintiff's claims for class-wide treatment are appropriate because all elements of Fed. R. Civ. P. 23(a) and (b)(2)-(3) are satisfied. Plaintiff can prove the elements of his claims on a class-wide basis using the same evidence as would be used to prove those elements in individual actions alleging the same claims.

91. **Numerosity:** All requirements of Fed. R. Civ. P. 23(a)(1) are satisfied. The members of the Classes are so numerous and geographically dispersed that individual joinder of all Class members is impracticable. While Plaintiff is informed and believe that there are likely at least hundreds of thousands of members of the Classes according to news reports, the precise number of Class members is unknown to Plaintiff. Class members may be identified through objective means including Postmeds' own records. Class members may be notified of the pendency of this action by recognized, court-approved notice dissemination methods, which may include U.S. mail, electronic mail, internet postings, and/or published notice.

92. **Commonality and Predominance:** All requirements of Fed. R. Civ. P. 23(a)(2) and 23(b)(3) are satisfied. This action involves common questions of law and fact, which predominate over any questions affecting individual Class members, including, without limitation:

a. Whether Defendant owed a duty to Plaintiff and Class members to secure and safeguard their e-PHI;

b. Whether Defendant failed to use reasonable care and reasonable methods to secure and safeguard Plaintiff's and Class members' e-PHI;

c. Whether Defendant properly implemented security measures as required by HIPAA or any other laws or industry standards to protect Plaintiff's and Class members' e-PHI from unauthorized access, capture, dissemination and misuse;

d. Whether Plaintiff and members of the Class were injured and suffered damages and ascertainable losses as a result of Defendant's actions or failure to act;

e. Whether Defendant engaged in active misfeasance and misconduct alleged herein;

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

g. Whether Defendant's failure to provide adequate security proximately caused Plaintiff's and Class members' injuries; and

h. Whether Plaintiff and Class members are entitled to declaratory and injunctive relief.

93. **Typicality:** All requirements of Fed. R. Civ. P. 23(a)(3) are satisfied. Plaintiff is a member of the Classes. Plaintiff's claims are typical of the claims of all Class members because Plaintiff, like other Class members, suffered theft of his e-PHI.

94. **Adequacy of Representation:** All requirements of Fed. R. Civ. P. 23(a)(4) are satisfied. Plaintiff is an adequate Class representative because he is a member of the Classes and his interests do not conflict with the interests of other Class members that he seeks to represent. Plaintiff is committed to pursuing this matter for the Classes with the Class's collective best interest in mind. Plaintiff has retained counsel competent and experienced in complex class action

litigation of this type and Plaintiff intends to prosecute this action vigorously. Plaintiff, and his counsel, will fairly and adequately protect the Class's interests.

95. **Predominance and Superiority:** All requirements of Fed. R. Civ. P. 23(b)(3) are satisfied. As described above, common issues of law or fact predominate over individual issues. Resolution of those common issues in Plaintiff's case will also resolve them for the Class's claims. In addition, a class action is superior to any other available means for the fair and efficient adjudication of this controversy and no unusual difficulties are likely to be encountered in the management of this class action. The damages or other financial detriment suffered by Plaintiff and other Class members are relatively small compared to the burden and expense that would be required to individually litigate their claims against Postmeds, so it would be impracticable for members of the Class to individually seek redress for Defendant's wrongful conduct. Even if Class members could afford individual litigation, the court system could not. Individualized litigation creates a potential for inconsistent or contradictory judgments and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single court.

96. **Cohesiveness:** All requirements of Fed. R. Civ. P. 23(b)(2) are satisfied. Postmeds has acted, or refused to act, on grounds generally applicable to the Class such that final declaratory or injunctive relief appropriate.

97. Plaintiff reserves the right to revise the foregoing class allegations and definitions based on facts learned and legal developments following additional investigation, discovery, or otherwise.

CALIFORNIA LAW APPLIES TO THE ENTIRE CLASS

98. California's substantive laws apply to every member of the Class, regardless of where in the United States the Class member resides.

99. California's substantive laws may be constitutionally applied to the claims of Plaintiff and the Class under the Due Process Clause, 14th Amend. § 1, and the Full Faith and Credit Clause, Art. IV § 1 of the U.S. Constitution. California has significant contacts, or

significant aggregation of contacts, to the claims asserted by Plaintiff and all Class members, thereby creating state interests that ensure that the choice of California state law is not arbitrary or unfair.

100. Postmeds principal place of business is located in California. Postmeds also owns property and conducts substantial business in California, and therefore California has an interest in regulating Postmeds' conduct under its laws. Defendant's decision to reside in California and avail itself of California's laws, and to engage in the challenged conduct from and emanating out of California, renders the application of California law to the claims herein constitutionally permissible.

101. California is also the state from which Postmeds' alleged misconduct emanated. This conduct similarly injured and affected Plaintiff and all other Class members.

102. The application of California laws to the Class is also appropriate under California's choice of law rules because California has significant contacts to the claims of Plaintiff and the proposed Class and Subclasses, and California has a greater interest in applying its laws here than any other interested state.

CLAIMS FOR RELIEF

COUNT I

NEGLIGENCE

(On Behalf of the Nationwide Class)

103. Plaintiff re-alleges and incorporates by reference all preceding allegations as if fully set forth herein.

104. Postmeds provides fulfillment to pharmacies nationwide and collects sensitive e-PHI information, including Plaintiff and Class members, in connection with these services.

105. Given the highly sensitive nature of e-PHI and likelihood of harm resulting from its unauthorized access, acquisition, use, or disclosure, multiple statutes, regulations, and guidelines, in addition to the common law, impose a duty on Postmeds to protect this information.

106. For example, the HIPAA Security Rule requires Postmeds to: (a) ensure the confidentiality, integrity, and availability of all e-PHI they create, receive, maintain or transmit; (b) proactively identify and protect against reasonably anticipated threats to the security or

integrity of the information; (c) protect against reasonably anticipated, impermissible uses or disclosures; (d) put in place the required administrative, physical and technical safeguards; (e) implement policies and procedures to prevent, detect, contain, and correct security violations; (f) effectively train their workforce regarding the proper handling of e-PHI; and (g) designate individual security and privacy officers to ensure compliance.

107. Postmeds also had a duty to use reasonable data security measures under several state and federal laws, including § 5 of the FTC Act, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect consumer data.

108. Postmeds owed a duty of care to Plaintiff and Class members to provide data security consistent with the various statutory requirements, regulations, and other notices described above.

109. Accordingly, Postmeds owed a duty to Plaintiff and Class members to exercise reasonable care in safeguarding and protecting their highly sensitive and confidential e-PHI by, among other things: (a) maintaining adequate security systems to ensure that Plaintiff's and Class members' highly sensitive and confidential e-PHI was adequately secured and protected; (b) implementing processes that would detect a breach of Postmeds' systems in a timely manner; and (c) timely notifying patients, including Plaintiff and Class members, that their highly sensitive and confidential e-PHI had been accessed, acquired, used, or disclosed as a result of any data breach so that Plaintiff and Class members could protect themselves from identify theft by obtaining credit and/or identify theft monitoring protection, canceling or changing their bank account and/or debit or credit card information, and/or taking other appropriate precautions.

110. Postmeds' duty of care arose as a result of, among other things, the special relationship that existed between Postmeds and the users of its services via the pharmacies that transacted with it. Postmeds was the only party in a position to ensure that its systems were sufficient to protect against the foreseeable risk that an unauthorized access could occur, which would result in substantial harm to consumers.

111. Postmeds was subject to an "independent duty" untethered to any contract between Plaintiff and Class members and Defendant.

112. Postmeds breached its duty to exercise reasonable care in safeguarding and protecting Plaintiff's and Class members' highly sensitive and confidential e-PHI by failing to adopt, implement, and maintain adequate security measures.

113. For example, Postmeds failed to implement appropriate systems to detect any breach of their systems and allow unfettered access without any passwords. Postmeds negligently failed to abide by the HIPAA Security Rule, among other guidelines and regulations, by failing to protect against anticipated threats to the security or integrity of Plaintiff's and Class members' highly sensitive and confidential e-PHI, and any reasonably anticipated impermissible uses or disclosures of their highly sensitive and confidential e-PHI.

114. Postmeds also breached their duty to exercise reasonable care in safeguarding and protecting Plaintiff's and Class members' highly sensitive and confidential e-PHI by failing to timely notify Plaintiff and Class members that their highly sensitive and confidential e-PHI could be and had been accessed by unauthorized third parties.

115. Postmeds' failure to comply with industry regulations such as HIPAA further evidence their negligence in failing to exercise reasonable care in safeguarding and protecting Plaintiff's and Class members' highly sensitive and confidential e-PHI.

116. It was foreseeable to Postmeds' that a failure to use reasonable measures to protect its patients' highly sensitive and confidential e-PHI could result in injury to its patients.

117. Actual and attempted breaches of data security were reasonably foreseeable to Postmeds given that other health care facilities and keepers of e-PHI have recently been breached before as well as the known frequency of data breaches and various warnings from industry experts.

118. The injuries and harm suffered by Plaintiff and Class members as a result of having their highly sensitive and confidential e-PHI accessed, viewed, acquired, used, or disclosed without authorization was the reasonably foreseeable result of Postmeds' failure to exercise reasonable care in safeguarding and protecting Plaintiff's and Class members' highly sensitive and

confidential e-PHI. Postmeds knew or should have known that the systems and technologies used for storing Plaintiff's and Class members' highly sensitive and confidential e-PHI allowed that information to be accessed, acquired, used, or disclosed by unauthorized third parties. But for Defendant's wrongful and negligent breach of duties owed to Plaintiff and Class members, the injuries alleged herein would not have occurred.

119. In connection with the conduct described above, Postmeds acted wantonly, recklessly, and with complete disregard for the consequences Plaintiff and Class members would suffer if their highly sensitive and confidential e-PHI was accessed by unauthorized third parties.

120. In addition to Defendant's common law duty to exercise reasonable care in securing Plaintiff's and Class members' data, several statutes independently imposed a duty on Postmeds to safeguard highly sensitive e-PHI. Defendant's violation of these statutory duties, as described below, each independently provides an evidentiary presumption to support Plaintiff's and Class members' negligence claim as negligence *per se*.

HIPAA

121. As alleged above, the HIPAA Security Rule requires Postmeds to maintain reasonable and appropriate administrative, technical, and physical safeguards for protecting highly sensitive and confidential e-PHI, which Defendant negligently failed to implement.

122. The HIPAA Security Rule also requires Postmeds to protect against reasonably anticipated threats to the security or integrity of e-PHI and protect against reasonably anticipated impermissible uses or disclosures, which Postmeds negligently failed to do. *See* 45 C.F.R. Part 160 and Part 164, Subpart A and C.

123. Defendant's failure to secure Plaintiff's and Class members' e-PHI and to notify them that such information could be and had been accessed by unauthorized third parties violated at least the following HIPAA regulations:

a. The HIPAA Privacy and Security Rule 45 C.F.R. § 160 and 45 C.F.R. § 164, Subpart A, C, and E

   i. 45 C.F.R. § 164.306

   ii. 45 C.F.R. § 164.308

iii. 45 C.F.R. § 164.312

iv. 45 C.F.R. § 164.314

v. 45 C.F.R. § 164.502

vi. 45 C.F.R. § 164.530

124. The harm that has occurred is the type of harm that HIPAA was intended to guard against, namely, the disclosure of patients' sensitive patient information, including e-PHI.

125. Plaintiff and Class members are within the class of persons that the HIPAA Privacy and Security Rule were intended to protect, because the HIPAA Privacy and Security rule were expressly designed to protect sensitive patient information.

126. Postmeds had a duty to Plaintiff and Class members to implement and maintain reasonable security procedures and practices under HIPAA to safeguard Plaintiff's and Class members' highly sensitive and confidential e-PHI.

127. Defendant breached their duties to Plaintiff and Class members under the HIPAA, by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and Class members' highly sensitive and confidential e-PHI.

128. Postmeds' violations of HIPAA and its failure to comply with applicable laws and regulations constitutes negligence *per se*.

FTC Act, 15 U.S.C. § 45

129. As alleged above, pursuant to the FTC Act, 15 U.S.C. § 45, Postmeds had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiff's and Class members' highly sensitive and confidential e-PHI.

130. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the failure to use reasonable measures to protect highly sensitive and confidential e-PHI. The FTC publications and orders described above also form part of the basis of Postmeds' duty.

131. Postmeds violated Section 5 of the FTC Act by failing to use reasonable measures to protect highly sensitive and confidential e-PHI and comply with applicable industry standards, including the FTC Act, as described in detail herein. Defendant' conduct was particularly

unreasonable given the nature and amount of e-PHI it collected and stored and the foreseeable consequences of a data breach, including specifically, as described herein, the damages that would result to consumers.

132. Plaintiff and Class members are consumers within the class of persons Section 5 of the FTC Act was intended to protect because they paid for prescriptions via the pharmacies that Postmeds contracted with.

133. The harm that has occurred is the type of harm the FTC Act was intended to guard against, namely harm to consumers as a result of unfair practices in commerce.

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

135. Defendant had a duty to Plaintiff and Class members to implement and maintain reasonable security procedures and practices to safeguard Plaintiff's and Class members' highly sensitive and confidential e-PHI.

136. Postmeds breached their duties to Plaintiff and Class members under the FTC Act, by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and Class members' highly sensitive and confidential e-PHI.

137. Postmeds' violations of Section 5 of the FTC Act and its failure to comply with applicable laws and regulations constitutes negligence *per se*.

California's Confidentiality of Medical Information Act

Cal. Civ. Code § 56, *et seq.*

138. Under the CMIA, "[a]n electronic health record system or electronic medical record system shall do the following: (A) Protect and preserve the integrity of electronic medical information; [and] (B) Automatically record and preserve any change or deletion of any electronically stored medical information. The record of any change or deletion shall include the identity of the person who accessed and changed the medical information, the date and time the medical information was accessed, and the change that was made to the medical information." Cal. Civ. Code § 56.101(b)(1)(A) – (B).

139. Postmeds violated the CMIA by negligently maintaining, preserving, and storing Plaintiff's and Class members' medical information inasmuch as it did not implement adequate security protocols to prevent unauthorized access to medical information, maintain an adequate electronic security system to prevent data breaches, or employ industry standard and commercially viable measures to mitigate the risks of any data the risks of any data breach or otherwise comply with HIPAA data security requirements.

140. Defendant failed to protect and preserve the integrity of electronic medical information and automatically record and preserve any change or deletion of any electronically stored medical information.

141. Plaintiff and Class members are within the class of persons the CMIA is intended to protect against, namely, patients of health care providers and the associates of those providers.

142. The harm that has occurred is the type of harm the CMIA was intended to guard against, namely protecting and preserving the integrity of electronic medical information.

143. As a direct and proximate result of Defendant's negligence, Plaintiff's and Class members' medical information was accessible to exfiltrate by any unauthorized third-party bad actor and they were injured as a result.

144. The injury and harm suffered by Plaintiff and Class members was a reasonably foreseeable result of Postmeds' breach of its duties. Postmeds knew or should have known that the breach of its duties would cause Plaintiff and Class members to suffer the foreseeable harms associated with the exposure of their medical information.

145. Defendant's violations of the CMIA constitutes negligence *per se*.

146. As a direct and proximate result of Defendant's negligence, including violations of HIPAA, the FTC Act, and the CMIA constituting negligence *per se*, Plaintiff and Class members sustained damages, including violation of their privacy interest and emotional distress, as alleged herein. Plaintiff and Class members are entitled to compensatory and consequential damages suffered as a result of the incident.

147. As a result of Defendant's negligence, Plaintiff and Class members are also entitled to injunctive relief requiring Postmeds to, among other things: (i) strengthen its data security

systems and monitoring procedures; (ii) submit to future annual audits of those systems; and (iii) provide free credit monitoring and identity theft insurance to Plaintiff and all Class members.

COUNT II
BREACH OF IMPLIED CONTRACT
(On behalf of the Nationwide Class)

148. Plaintiff re-alleges and incorporates by reference all preceding allegations as if fully set forth herein.

149. When Plaintiff and Class members provided their highly sensitive and confidential e-PHI to Defendant in exchange for services, they entered into implied contracts with Postmeds under which Defendant agreed to take reasonable steps to protect their highly sensitive and confidential e-PHI.

150. Plaintiff and Class members were invited and solicited to provide their highly sensitive and confidential e-PHI as part of Postmeds' and the affiliated pharmacy's regular business practices. Plaintiff and Class members accepted Postmeds' offers and provided their highly sensitive and confidential e-PHI to Defendant.

151. When entering into the implied contracts, Plaintiff and Class members reasonably believed and expected that Postmeds' data security practices complied with relevant laws, regulations, and industry standards.

152. When entering into the implied contracts, Plaintiff and Class members reasonably believed that Defendant would safeguard and protect their highly sensitive and confidential e-PHI and that Postmeds would use part of the funds received from affiliated pharmacies, Plaintiff via the pharmacy and Class members via the pharmacy to pay for adequate and reasonable data security practices. Defendant failed to do so.

153. Plaintiff and Class members would not have provided their highly sensitive and confidential e-PHI to Postmeds in the absence of Postmeds' implied promise to keep their highly sensitive and confidential e-PHI reasonably secure.

154. Plaintiff and Class members fully performed their obligations under the implied contracts by paying for their prescriptions.

155. Postmeds breached its implied contracts with Plaintiff and Class members by failing to safeguard and protect their highly sensitive and confidential e-PHI.

156. As a direct and proximate result of Defendant's breaches of implied contracts, Plaintiff and Class members sustained damages as alleged herein, including when they received services that did not include reasonable security measures sufficient to protect Plaintiff's and Class members' highly sensitive and confidential e-PHI, despite Postmeds' promise that it would do so. Plaintiff and Class members would not have paid for and used, or would have paid less, for Postmeds' services via the pharmacies Postmeds' transacted with had they known these representations were false.

157. Plaintiff and Class members are also entitled to injunctive relief requiring Postmeds to, among other things: (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems; and (iii) provide free credit monitoring and identity theft insurance to all Class members.

COUNT III
COMMON LAW INVASION OF PRIVACY – INTRUSION UPON SECLUSION
(On behalf of the Nationwide Class)

158. Plaintiff re-alleges and incorporates by reference all preceding allegations as if fully set forth herein.

159. Plaintiff asserting claims for intrusion upon seclusion must plead (1) that the Defendant intentionally intruded into a matter as to which Plaintiff had a reasonable expectation of privacy; and (2) that the intrusion was highly offensive to a reasonable person.

160. There is no area where there is more of a reasonable expectation of privacy than in healthcare, which is the type of data maintained by Postmeds.

161. Postmeds intentionally intruded upon the solitude, seclusion and private affairs of Plaintiff and Class members by intentionally configuring their systems in such a way that left them vulnerable any unauthorized access to their systems, which compromised Plaintiff's and Class members' highly sensitive and confidential e-PHI. Only Postmeds had control over its systems.

162. Defendant's conduct is especially egregious and offensive as they failed to have any adequate security measures in place to prevent, track, or detect in a timely fashion unauthorized access to Plaintiff's and Class members' e-PHI.

163. At all times, Postmeds was aware that Plaintiff's and Class members' highly sensitive and confidential e-PHI in their possession contained highly sensitive medical information, including name, prescription information, medication type, prescribing physician, and demographic information.

164. Plaintiff and Class members have a reasonable expectation in their e-PHI, which contains highly sensitive medical information.

165. Postmeds intentionally configured their systems in such a way that stored Plaintiff's and Class Members' highly sensitive and confidential e-PHI to be left vulnerable to unauthorized access without regard for Plaintiff's and Class members' privacy interests.

166. The disclosure of the highly sensitive and confidential e-PHI was highly offensive to Plaintiff and Class members because it violated expectations of privacy that have been established by general social norms, including by granting access to information and data that is private and would not otherwise be disclosed.

167. Surveys consistently show that individuals care about the security and privacy of their highly sensitive and confidential e-PHI. In 2013, the *Office of the National Coordinator for Health Information Technology* found that 7 out of 10 individuals are concerned about the privacy of their medical records. The same study found that 3 out of 4 individuals are concerned about the security of their medical records. Likewise, a *Gallup* survey found that 78%of adults believe that it is very important that their medical records be kept confidential, and a majority of respondents believe no one should be permitted to see their records without consent. Plaintiff and Class members acted consistent with these polls and surveys by safeguarding their medical information, including the ePHI exfiltrated and stolen in the data breach.

168. Postmeds' conduct would be highly offensive to a reasonable person in that it violated statutory and regulatory protections designed to protect highly sensitive medical information, in addition to social norms. Defendant's conduct would be especially egregious to a

reasonable person as Postmeds publicly disclosed Plaintiff's and Class members' highly sensitive and confidential e-PHI without their consent, to any number of unauthorized persons, hackers and/or bad actors.

169. As a result of Defendant's actions, Plaintiff and Class members have suffered harm and injury, including but not limited to an invasion of their privacy rights.

170. Plaintiff and Class members have been damaged as a direct and proximate result of Postmeds' intrusion upon seclusion and are entitled to just compensation.

171. Plaintiff and Class members are entitled to appropriate relief, including compensatory damages for the harm to their privacy, loss of valuable rights and protections, and heightened risk of future invasions of privacy.

COUNT IV
INVASION OF PRIVACY
ART. I, SEC 1 OF THE CALIFORNIA CONSTITUTION
(On behalf of the Nationwide Class and California Subclass)

172. Plaintiff re-alleges and incorporates by reference all preceding allegations as if fully set forth herein.

173. Art. I, § 1 of the California Constitution provides: "All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and privacy." Art. I, § 1, Cal. Const.

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

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

176. Postmeds violated Plaintiff's and California Subclass members' constitutional right to privacy by collecting, storing, and disclosing (1) e-PHI in which they had a legally protected privacy interest, (2) Plaintiff's and California Subclass members' e-PHI in which they had a

reasonable expectation of privacy in, (3) in a manner that was highly offensive to Plaintiff and California Subclass members, would be highly offensive to a reasonable person, and was in egregious violation of social norms.

177. Postmeds has intruded upon Plaintiff's and California Subclass members' legally protected privacy interests, including, *inter alia*: (i) interests in precluding the dissemination or misuse of sensitive and confidential personal—the e-PHI; and (ii) interests in making intimate personal healthcare decisions or conducting personal activities without observation, intrusion, or interference.

178. The highly sensitive and confidential e-PHI, which Postmeds stored, monitored, collected, and disclosed without Plaintiff's and California Subclass members' authorization and/or consent included, *inter alia*, including name, prescription information, medication type, demographic information, and prescribing physician.

179. Plaintiff and California Subclass members had a legally protected informational privacy interest in the confidential and sensitive e-PHI involved as well as a privacy interest in conducting their personal healthcare decisions and activities without intrusion, interference, or disclosure.

180. Defendant's actions constituted a serious invasion of privacy that would be highly offensive to a reasonable person in that: (i) the invasion occurred within a zone of privacy protected by the California Constitution, namely the misuse of information gathered for an improper purpose; and (ii) the invasion deprived Plaintiff and California Subclass members of the ability to control the circulation of their highly sensitive and confidential e-PHI, which is considered fundamental to the right to privacy.

181. Plaintiff and California Subclass members had a reasonable expectation of privacy in that: (i) Postmeds' invasion of privacy occurred as a result of Postmeds' security practices including the collecting, storage, and unauthorized disclosure of highly sensitive and confidential e-PHI; (ii) Plaintiff and California Subclass members did not consent or otherwise authorize Postmeds to disclose their highly sensitive and confidential e-PHI; and (iii) Plaintiff and California

Subclass members could not reasonably expect Postmeds would commit acts in violation of laws protecting privacy.

182. As a result of Defendant's actions, Plaintiff and California Subclass members have been damaged as a direct and proximate result of Postmeds' invasion of their privacy and are entitled to just compensation.

183. Plaintiff and California Subclass members suffered actual and concrete injury as a result of Defendant's violations of their privacy interests. Plaintiff and California Subclass members are entitled to appropriate relief, including damages to compensate them for the harm to their privacy interests, loss of valuable rights and protections, heightened risk of future invasions of privacy, and the mental and emotional distress and harm to human dignity interests caused by Defendant's invasions.

184. Plaintiff and the California Subclass seek appropriate relief for that injury, including but not limited to damages that will reasonably compensate Plaintiff and California Subclass members for the harm to their privacy interests as well as any disgorgement of profits made by Postmeds as a result of its intrusions upon Plaintiff's and California Subclass members' privacy.

COUNT V
VIOLATION OF THE CALIFORNIA UNFAIR COMPETITION LAW
Cal. Bus. & Prof. Code § 17200, *et seq.*
(On Behalf of the California Subclass)

185. Plaintiff re-alleges and incorporates by reference all preceding allegations as if fully set forth herein.

186. Postmeds is a "person" as defined by Cal. Bus. & Prof. Code §17201.

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

188. Postmeds' business acts and practices are "unlawful" under the Unfair Competition Law, Cal. Bus. & Prof. Code §§ 17200 *et. seq.* ("UCL"), because, as alleged above, Defendant violated the California common law, California Constitution, and the other state and federal statutes and causes of action described herein.

189. Postmeds business acts and practices are "unfair" under the UCL, because, as alleged above, California has a strong public policy of protecting consumers' privacy interests, including protecting consumers' personal data, including highly sensitive and confidential e-PHI. Defendant violated this public policy by, among other things, surreptitiously collecting, storing, disclosing, and otherwise misusing Plaintiff's and California Subclass members' highly sensitive and confidential e-PHI without Plaintiff's and California Subclass members' consent. Postmeds further engaged in unfair business practices because it made material misrepresentations and omissions concerning the information that Postmeds assured patients it would protect their highly sensitive and confidential e-PHI, which deceived and misled patients. Defendant's conduct violates the policies of the statutes referenced herein.

190. Postmeds' business acts and practices are also "unfair" in that they are immoral, unethical, oppressive, unscrupulous, and/or substantially injurious to consumers. The gravity of the harm of Postmeds' collecting, storing, disclosing, and otherwise misusing Plaintiff's and California Subclass members' highly sensitive and confidential e-PHI is significant, and there is no corresponding benefit resulting from such conduct. Finally, because Plaintiff and California Subclass members were completely unaware of Defendant's conduct, they could not have possibly avoided the harm.

191. Postmeds' business acts and practices are also "fraudulent" within the meaning of the UCL. Defendant misrepresented that it maintained sufficient data security measures and systems to protect Plaintiff's and California Subclass members' e-PHI. Postmeds never disclosed that these practices were severely deficient.

192. Postmeds' unlawful, unfair, and deceptive acts and practices include:

(a) Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's and California Subclass members' e-PHI, which was a direct and proximate cause of the incident with advised of the unfettered access to e-PHI and omitting, suppressing, and concealing the material fact of that failure;

(b) Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following well-publicized cybersecurity incidents;

(c) Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and California Subclass members' e-PHI, including duties imposed by the FTC Act, HIPAA, and CMIA which was a direct and proximate cause of the incident and omitting, suppressing, and concealing the material fact of that failure;

(d) Misrepresenting that it would protect the privacy and confidentiality of Plaintiff's and California Subclass members' e-PHI, including by implementing and maintaining reasonable security measures;

(e) Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and California Subclass members' e-PHI, including duties imposed by the FTC Act, HIPAA, and CMIA;

(f) Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff's and California Subclass members' e-PHI; and

(g) Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and California Subclass members' e-PHI, including duties imposed by the FTC Act, HIPAA, and the CMIA.

193. Postmeds' representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendant's data security and ability to protect the confidentiality of consumers' highly sensitive and confidential e-PHI.

194. As a direct and proximate result of Defendant's unfair, unlawful, and fraudulent acts and practices, Plaintiff and California Subclass members were injured and lost money or property, i.e., the loss of the benefit of their bargain with Postmeds and the pharmacies Postmeds transacted with as they would not have paid those pharmacies for goods and services or would have paid less for such goods and services; costs to be spent for credit monitoring and identity

protection services; time and expenses related to monitoring their financial accounts for fraudulent activity; loss of value of their highly sensitive and confidential e-PHI; and an increased, imminent risk of fraud and identity theft.

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

196. Plaintiff and California Subclass members would not have paid for goods with the pharmacies which Postmeds is a vendor, or would have paid significantly less, had they known that its representations and omissions concerning data security were false.

197. Plaintiff and California Subclass members have lost money and property as a result of Postmeds' conduct in violation of the UCL, as stated in herein and above. Health data, such as the e-PHI collected by Defendant, objectively has value. For instance, Pfizer annually pays approximately $12 million to purchase health data from various sources.

198. Consumers and patients, including Plaintiff and California Subclass members also value their health data. According to the annual Financial Trust Index Survey, conducted by *the University of Chicago's Booth School of Business and Northwestern University's Kellogg School of Management*, which interviewed more than 1,000 Americans, 93%would not share their health data with a digital platform for free. Half of the survey respondents would only share their data for $100,000 or more, and 22% would only share their data if they received between $1,000 and $100,000.

199. By deceptively storing, collecting, and disclosing this highly sensitive and confidential e-PHI, Postmeds has taken money or property from Plaintiff and California Subclass members.

200. Plaintiff and California Subclass members seek all monetary and non-monetary relief allowed by law, including compensatory damages; restitution; disgorgement; punitive damages; injunctive relief; and reasonable attorneys' fees and costs.

COUNT VI
VIOLATION OF THE CALIFORNIA CONFIDENTIALITY OF MEDICAL INFORMATION ACT,
Cal. Civ. Code § 56, *et seq.*
(On Behalf of the California Subclass)

201. Plaintiff re-alleges and incorporates by reference all preceding allegations as if fully set forth herein.

202. Under the CMIA, "medical information" is defined as "any individually identifiable information, in electronic or physical form, in possession of or derived from a provider of health care, health care service plan, pharmaceutical company, or contractor regarding a patient's medical history, mental or physical condition, or treatment. "Individually identifiable" means that the medical information includes or contains any element of personal identifying information sufficient to allow identification of the individual, such as the patient's name, address, electronic mail address, telephone number, or social security number, or other information that, alone or in combination with other publicly available information, reveals the individual's identity." Cal. Civ. Code § 56.05(j). Plaintiff's and California Subclass members' highly sensitive and confidential e-PHI constitutes "medical information" under the CMIA because it contained individually identifiable information in the possession or derived from Postmeds.

203. Postmeds as a "contractor" is subject to the CMIA, because it is a "business organized for the purpose of maintaining medical information, as defined in subdivision (j) of Section 56.05, in order to make the information available to an individual or to a provider of health care at the request of the individual or a provider of health care, for purposes of allowing the individual to manage his or her information, or for the diagnosis and treatment of the individual, shall be deemed to be a provider of health care subject to the requirements of this part." Cal. Civ. Code § 56.06(a). As such, Postmeds is subject to the penalties for improper use and disclosure of medical information prescribed in this part." Cal. Civ. Code § 56.06(e).

204. Postmeds is also subject to the CMIA, because it is a "business that offers software or hardware to consumers, including a mobile application or other related device that is designed to maintain medical information, as defined in subdivision (j) of Section 56.05, in order to make the information available to an individual or provider of health care at the request of the individual or provider of healthcare, for purposes of allowing the individual to manage his or her information, or for the diagnosis, treatment, or management of a medical condition of the individual." Cal. Civ. Code § 56.06(b).

205. Under the CMIA, "patient" means "any natural person, whether or not still living, who received health care services from a provider of health care and to whom medical information pertains. Cal. Civ. Code § 56.05(k)." Plaintiff and California Subclass members are "patients" under the CMIA.

206. Under the CMIA, "authorized recipient" means "any person who is authorized to receive medical information pursuant to Section 56.10 or 56.20. Cal. Civ. Code § 56.05(b)." Postmeds is an "authorized recipient" under the CMIA.

207. Postmeds stored in electronic form on its cloud Plaintiff's and California Subclass members' "medical information" as defined by Cal. Civ. Code § 56.05(j).

208. Under the CMIA, "[a] provider of health care, health care service plan, or contractor shall not disclose medical information regarding a patient of the provider of health care or an enrollee or subscriber of a health care service plan without first obtaining an authorization, except as provided in subdivision (b) or (c)." Cal. Civ. Code § 56.10(a).

209. Postmeds violated Cal. Civ. Code § 56.10(a) as Plaintiff and California Subclass members did not provide Postmeds authorization nor was Postmeds otherwise authorized to disclose Plaintiff's or California Subclass members' medical information to any unauthorized third-party.

210. As a direct and proximate result of Defendant's violation of Cal. Civ. Code Section 56.10(a), Plaintiff's, and California Subclass members' medical information was viewed by a number of unauthorized third parties.

211. Postmeds' unauthorized disclosures of Plaintiff's and California Subclass members' medical information has caused injury to Plaintiff and California Subclass members.

212. In addition, Cal. Civil Code Section 56.101, subdivision (a), requires that every provider of health care "who creates, maintains, preserves, stores, abandons, destroys, or disposes of medical information shall do so in a manner that preserves the confidentiality of the information contained therein."

213. Further, "[a]n electronic health record system or electronic medical record system shall do the following:(A) Protect and preserve the integrity of electronic medical information;

[and] (B) Automatically record and preserve any change or deletion of any electronically stored medical information. The record of any change or deletion shall include the identity of the person who accessed and changed the medical information, the date and time the medical information was accessed, and the change that was made to the medical information." Cal. Civ. Code § 56.101(b)(1)(A) – (B).

214. Postmeds failed to maintain, preserve, and store medical information in a manner that preserves the confidentiality of the information contained therein because it disclosed to third parties Plaintiff's and California Subclass members' highly sensitive and confidential e-PHI without consent.

215. As described throughout this Complaint, Postmeds also violated Cal. Civ. Code § 56.101(a) by negligently maintaining, preserving, and storing Plaintiff's and California Subclass members' medical information inasmuch as it did not implement adequate security protocols to prevent unauthorized access to medical information, maintain an adequate electronic security system to prevent data breaches, or employ industry standard and commercially viable measures to mitigate the risks of any data the risks of any data breach or otherwise comply with HIPAA data security requirements.

216. Postmeds failed to protect and preserve the integrity of electronic medical information and automatically record and preserve any change or deletion of any electronically stored medical information.

217. As a direct and proximate result of Defendant's violation of Cal. Civ. Code Section 56.101(a), Plaintiff's, Nationwide class members' and California Subclass members' medical information was viewed by a number of unauthorized third parties.

218. Postmeds' negligent maintenance, preservation, and storage of Plaintiff's and California Subclass members' medical information has caused injury to Plaintiff and California Subclass members.

219. Accordingly, Plaintiff and California Subclass members are entitled to: (1) nominal damages of $1,000 per violation; (2) actual damages, in an amount to be determined at trial; (3)

statutory damages pursuant to 56.36(c); (4) punitive damages pursuant to Cal. Civ. Code Section 56.35; and (5) reasonable attorneys' fees and other litigation costs reasonably incurred.

COUNT VII
REQUEST FOR RELIEF UNDER THE DECLARATORY JUDGMENT ACT
28 U.S.C. § 2201, *et seq.*
(On Behalf of the Nationwide Class)

220. Plaintiff re-alleges and incorporates by reference all preceding allegations as if fully set forth herein.

221. Under the Declaratory Judgment Act, 28 U.S.C. § 2201, *et seq*., this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the statutes described in this Complaint.

222. An actual controversy has arisen in the wake of the data breach regarding Postmeds' present and prospective common law and statutory duties to reasonably safeguard its patients' highly sensitive and confidential e-PHI and whether Postmeds is currently maintaining data security measures adequate to protect Plaintiff and Class members from further data breaches. Plaintiff alleges that Defendant's data security practices remain inadequate.

223. Plaintiff and Class members continue to suffer injury as a result of the compromise of their highly sensitive and confidential e-PHI and remain at imminent risk that further compromises of their personal information will occur in the future.

224. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring that Postmeds continues to owe a legal duty to secure consumers' highly sensitive and confidential e-PHI, to timely notify consumers of any data breach, and to establish and implement data security measures that are adequate to secure its patients' highly sensitive and confidential e-PHI.

225. The Court also should issue corresponding prospective injunctive relief requiring Postmeds to employ adequate security protocols consistent with law and industry standards to protect patients' highly sensitive and confidential e-PHI.

226. If an injunction is not issued, Plaintiff and Class members will suffer irreparable injury, for which they lack an adequate legal remedy. The threat of another data breach is real,

immediate, and substantial. If another breach at Postmeds occurs, Plaintiff and Class members will not have an adequate remedy at law, because many of the resulting injuries are not readily quantified and they will be forced to bring multiple lawsuits to rectify the same conduct.

227. The hardship to Plaintiff and Class members if an injunction does not issue greatly exceeds the hardship to Postmeds if an injunction is issued. If another data breach incident occurs at Postmeds, Plaintiff and Class members will likely be subjected to substantial identify theft and other damages. On the other hand, the cost to Postmeds of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Defendant has a pre-existing legal obligation to employ such measures.

228. Issuance of the requested injunction will serve the public interest by preventing another data breach incident at Postmeds, thus eliminating the additional injuries that would result to Plaintiff and the millions of consumers whose confidential information would be further compromised.

COUNT VIII
VIOLATION OF THE CALIFORNIA CONSUMER PRIVACY ACT
Cal. Civ. Code § 1798.100 *et seq.*
(On Behalf of the California Subclass)

229. Plaintiff re-alleges and incorporates by reference all preceding allegations as if fully set forth herein.

230. Postmeds violated Section 1798.150 of the California Consumer Privacy Act by failing to prevent Plaintiff and the California Subclass members' nonencrypted and nonredacted e-PHI from unauthorized access and exfiltration, theft, or disclosure as a result of Defendant's violation of its duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information.

231. Postmeds knew or should have known that its data security practices were inadequate to secure California Subclass members' e-PHI and that its inadequate data security practices gave rise to the risk of a data breach.

232. Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature of the personal information it collected and stored.

233. Postmeds is a business that collects consumers' personal information, as defined by Cal. Civ. Code §§ 1798.100, *et seq*.

234. Plaintiff seeks injunctive relief in the form of an order requiring Postmeds to employ adequate security practices consistent with law and industry Postmeds to protect the California Subclass members' personal information, requiring Postmeds to complete its investigation, and to issue an amended statement giving a detailed explanation that confirms, with reasonable certainty, what categories of data were stolen and/or accessed without the California Subclass members' authorization, along with an explanation of how this incident occurred.

235. Plaintiff presently seeks only injunctive relief and any other relief the Court may deem proper pursuant to this section. Prior to initiating a claim for statutory damages, Plaintiff served written notice identifying Defendant's violations of Cal. Civil Code § 1798.150(a) and demanding the data breach incident be cured. If within 30 days Postmeds has not cured, Plaintiff will amend this Complaint to seek statutory damages pursuant to Cal. Civil Code § 1798.150(a)(1)(A).

RELIEF REQUESTED

Plaintiff, on behalf of all others similarly situated, request that the Court enter judgment against Defendant including the following:

A. Determining that this matter may proceed as a class action and certifying the Classes asserted herein;

B. Appointing Plaintiff as representative of the applicable Classes and appointing Plaintiff's counsel as Class counsel;

C. An award to Plaintiff and the Classes of compensatory, consequential, nominal, statutory, and treble damages as set forth above;

D. Ordering injunctive relief requiring Defendant to, among other things: (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems; (iii) provide several years of free credit monitoring and identity theft insurance to all Class members; and (iv) timely notify consumers of any future data breaches;

E. Entering a declaratory judgment stating that Defendant owes a legal duty to secure consumers' e-PHI, to timely notify patients of any data breach, and to establish and implement data security measures that are adequate to secure patients' e-PHI;

F. An award of attorneys' fees, costs, and expenses, as provided by law or equity;

G. An award of pre-judgment and post-judgment interest, as provided by law or equity; and

H. Such other relief as the Court may allow.

DEMAND FOR JURY TRIAL

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

Dated: November 10, 2023

/s/ Ronald A. Marron
Ronald A. Marron (175650)
Alexis M. Wood (270200)
Kas L. Gallucci (288709)
LAW OFFICES OF RONALD A. MARRON
651 Arroyo Drive
San Diego, CA 92103
Tel: (619) 696-9006
Fax: (619) 564-6665
ron@consumersadvocates.com
alexis@consumersadvocates.com
kas@consumersadvocates.com

Attorneys for Plaintiff and the Proposed Classes

EXHIBIT A

Postmeds, Inc.
Secure Processing Center
P.O. Box 3826
Suwanee, GA 30024

<<Name1>>
<<Address>>
<<Address 2>>
<<City>>, <<State>><<Zip>>
<<Country>>

<<Date>>

Dear <<Name1>>,

Postmeds, Inc. is a pharmacy company that fulfills prescription orders. At Postmeds, we are committed to providing outstanding pharmacy services and protecting the information in our care. We recently identified and addressed a cybersecurity incident involving some of that information and wanted to share with you what happened and the steps we are taking in response.

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

What Information was Involved: Our investigation determined that the bad actor accessed the files between August 30, 2023 to September 1, 2023. One or more of those files contained your name and prescription information. The information varied by individual, but may have included medication type, demographic information, and/or prescribing physician. Importantly, your Social Security number was **not** involved, as Postmeds does not receive this information.

What We Are Doing and What You Can Do in Response: We want you to know that we are taking this incident very seriously and regret any inconvenience or concern this may cause you. We are enhancing our security protocols and technical safeguards in response to this incident, and we are increasing awareness of cybersecurity threats through additional employee training. We also encourage you to regularly review your information for accuracy, as a best practice, including information you receive from your healthcare providers.

For more information: If you have additional questions about this incident, please call our dedicated, confidential call center at 1-855-457-9143, Monday through Friday, 9:00 a.m. to 9:00 p.m. Eastern Time.

Sincerely,

Postmeds, Inc.

CIVIL COVER SHEET

The JS-CAND 44 civil cover sheet and the information contained herein neither replace nor supplement the filing and service of pleadings or other papers as required by law, except as provided by local rules of court. This form, approved in its original form by the Judicial Conference of the United States in September 1974, is required for the Clerk of Court to initiate the civil docket sheet. *(SEE INSTRUCTIONS ON NEXT PAGE OF THIS FORM.)*

I. (a) PLAINTIFFS

Christopher Williams, individually and on behalf of all others similarly situated,

(b) County of Residence of First Listed Plaintiff Los Angeles
(EXCEPT IN U.S. PLAINTIFF CASES)

(c) Attorneys *(Firm Name, Address, and Telephone Number)*

Law Offices of Ronald A. Marron: 651 Arroyo Drive San Diego, CA 92103 (619) 696-9006

DEFENDANTS

Postmeds, Inc. d/b/a TruePill

County of Residence of First Listed Defendant
(IN U.S. PLAINTIFF CASES ONLY)

NOTE: IN LAND CONDEMNATION CASES, USE THE LOCATION OF THE TRACT OF LAND INVOLVED.

Attorneys *(If Known)*

II. BASIS OF JURISDICTION *(Place an "X" in One Box Only)*

- ☐ 1 U.S. Government Plaintiff
- ☒ 3 Federal Question *(U.S. Government Not a Party)*
- ☐ 2 U.S. Government Defendant
- ☐ 4 Diversity *(Indicate Citizenship of Parties in Item III)*

III. CITIZENSHIP OF PRINCIPAL PARTIES *(Place an "X" in One Box for Plaintiff and One Box for Defendant)*

(For Diversity Cases Only)

	PTF	DEF		PTF	DEF
Citizen of This State	☐ 1	☐ 1	Incorporated *or* Principal Place of Business In This State	☐ 4	☐ 4
Citizen of Another State	☐ 2	☐ 2	Incorporated *and* Principal Place of Business In Another State	☐ 5	☐ 5
Citizen or Subject of a Foreign Country	☐ 3	☐ 3	Foreign Nation	☐ 6	☐ 6

IV. NATURE OF SUIT *(Place an "X" in One Box Only)*

CONTRACT
- ☐ 110 Insurance
- ☐ 120 Marine
- ☐ 130 Miller Act
- ☐ 140 Negotiable Instrument
- ☐ 150 Recovery of Overpayment Of Veteran's Benefits
- ☐ 151 Medicare Act
- ☐ 152 Recovery of Defaulted Student Loans (Excludes Veterans)
- ☐ 153 Recovery of Overpayment of Veteran's Benefits
- ☐ 160 Stockholders' Suits
- ☐ 190 Other Contract
- ☐ 195 Contract Product Liability
- ☐ 196 Franchise

REAL PROPERTY
- ☐ 210 Land Condemnation
- ☐ 220 Foreclosure
- ☐ 230 Rent Lease & Ejectment
- ☐ 240 Torts to Land
- ☐ 245 Tort Product Liability
- ☐ 290 All Other Real Property

TORTS

PERSONAL INJURY
- ☐ 310 Airplane
- ☐ 315 Airplane Product Liability
- ☐ 320 Assault, Libel & Slander
- ☐ 330 Federal Employers' Liability
- ☐ 340 Marine
- ☐ 345 Marine Product Liability
- ☐ 350 Motor Vehicle
- ☐ 355 Motor Vehicle Product Liability
- ☐ 360 Other Personal Injury
- ☐ 362 Personal Injury -Medical Malpractice

PERSONAL INJURY
- ☐ 365 Personal Injury – Product Liability
- ☐ 367 Health Care/ Pharmaceutical Personal Injury Product Liability
- ☐ 368 Asbestos Personal Injury Product Liability

PERSONAL PROPERTY
- ☐ 370 Other Fraud
- ☐ 371 Truth in Lending
- ☐ 380 Other Personal Property Damage
- ☐ 385 Property Damage Product Liability

CIVIL RIGHTS
- ☐ 440 Other Civil Rights
- ☐ 441 Voting
- ☐ 442 Employment
- ☐ 443 Housing/ Accommodations
- ☐ 445 Amer. w/Disabilities–Employment
- ☐ 446 Amer. w/Disabilities–Other
- ☐ 448 Education

PRISONER PETITIONS

HABEAS CORPUS
- ☐ 463 Alien Detainee
- ☐ 510 Motions to Vacate Sentence
- ☐ 530 General
- ☐ 535 Death Penalty

OTHER
- ☐ 540 Mandamus & Other
- ☐ 550 Civil Rights
- ☐ 555 Prison Condition
- ☐ 560 Civil Detainee–Conditions of Confinement

FORFEITURE/PENALTY
- ☐ 625 Drug Related Seizure of Property 21 USC § 881
- ☐ 690 Other

LABOR
- ☐ 710 Fair Labor Standards Act
- ☐ 720 Labor/Management Relations
- ☐ 740 Railway Labor Act
- ☐ 751 Family and Medical Leave Act
- ☐ 790 Other Labor Litigation
- ☐ 791 Employee Retirement Income Security Act

IMMIGRATION
- ☐ 462 Naturalization Application
- ☐ 465 Other Immigration Actions

BANKRUPTCY
- ☐ 422 Appeal 28 USC § 158
- ☐ 423 Withdrawal 28 USC § 157

PROPERTY RIGHTS
- ☐ 820 Copyrights
- ☐ 830 Patent
- ☐ 835 Patent—Abbreviated New Drug Application
- ☐ 840 Trademark
- ☐ 880 Defend Trade Secrets Act of 2016

SOCIAL SECURITY
- ☐ 861 HIA (1395ff)
- ☐ 862 Black Lung (923)
- ☐ 863 DIWC/DIWW (405(g))
- ☐ 864 SSID Title XVI
- ☐ 865 RSI (405(g))

FEDERAL TAX SUITS
- ☐ 870 Taxes (U.S. Plaintiff or Defendant)
- ☐ 871 IRS–Third Party 26 USC § 7609

OTHER STATUTES
- ☐ 375 False Claims Act
- ☐ 376 Qui Tam (31 USC § 3729(a))
- ☐ 400 State Reapportionment
- ☐ 410 Antitrust
- ☐ 430 Banks and Banking
- ☐ 450 Commerce
- ☐ 460 Deportation
- ☐ 470 Racketeer Influenced & Corrupt Organizations
- ☐ 480 Consumer Credit
- ☐ 485 Telephone Consumer Protection Act
- ☐ 490 Cable/Sat TV
- ☐ 850 Securities/Commodities/ Exchange
- ☒ 890 Other Statutory Actions
- ☐ 891 Agricultural Acts
- ☐ 893 Environmental Matters
- ☐ 895 Freedom of Information Act
- ☐ 896 Arbitration
- ☐ 899 Administrative Procedure Act/Review or Appeal of Agency Decision
- ☐ 950 Constitutionality of State Statutes

V. ORIGIN *(Place an "X" in One Box Only)*

☒ 1 Original Proceeding ☐ 2 Removed from State Court ☐ 3 Remanded from Appellate Court ☐ 4 Reinstated or Reopened ☐ 5 Transferred from Another District *(specify)* ☐ 6 Multidistrict Litigation–Transfer ☐ 8 Multidistrict Litigation–Direct File

VI. CAUSE OF ACTION

Cite the U.S. Civil Statute under which you are filing ***(Do not cite jurisdictional statutes unless diversity)***:
Declaratory Relief, Negligence, HIPPA, FTC Act, Breach of Implied Contract, Invasion of Privacy

Brief description of cause:
Data Breach Class Action for Negligence, Invasion of Privacy, Violations of HIPPA, Breach of Contract, and state class action claims

VII. REQUESTED IN COMPLAINT:

✓ CHECK IF THIS IS A **CLASS ACTION** UNDER RULE 23, Fed. R. Civ. P.

DEMAND $

CHECK YES only if demanded in complaint:
JURY DEMAND: ☒ Yes ☐ No

VIII. RELATED CASE(S), IF ANY *(See instructions):*

JUDGE See Attached DOCKET NUMBER See Attached

IX. DIVISIONAL ASSIGNMENT (Civil Local Rule 3-2)

(Place an "X" in One Box Only) ☒ **SAN FRANCISCO/OAKLAND** ☐ **SAN JOSE** ☐ **EUREKA-MCKINLEYVILLE**

DATE 11/10/2023 **SIGNATURE OF ATTORNEY OF RECORD** s/ Ronald A. Marron

Related Cases

Docket No. 3:23-cv-05710-SK; Hon. Sallie Kim

Docket No. 4:23-cv-05726-DMR Hon. Donna M. Ryu

Docket No. 4:23-cv-05732-KAW Hon. Kandis A. Westmore

Docket No. 4:23-cv-05743-KAW Hon. Kandis A. Westmore

Docket No. 3:23-cv-05772-TSH Hon. Thomas S. Hixon