IN THE UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF KENTUCKY

TANDRIA MARALLO, individually and on behalf of all others similarly situated, Plaintiff, v. PHARMERICA CORPORATION and RES-CARE, INC., d/b/a BRIGHTSPRING HEALTH SERVICES, Defendants.	Case No. 3:23CV-298-CHB **CLASS ACTION** **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Plaintiff Tandria Marallo ("Plaintiff"), individually, and on behalf of all others similarly situated (collectively, "Class members"), by and through her attorneys, bring this Class Action Complaint against Defendants PharMerica Corporation ("PharMerica") and Res-Care, Inc., d/b/a BrightSpring Health Services ("BrightSpring" and together with PharMerica "Defendants"), and complains and alleges upon personal knowledge as to herself and information and belief as to all other matters.

INTRODUCTION

1. Plaintiff brings this class action against Defendants for their failure to secure and safeguard her and approximately 5,815,591 other individuals' personally identifying information ("PII") and personal health information ("PHI"), including names, dates of birth, Social Security numbers, medication information, and health insurance information.

2. PharMerica provides pharmacy services across a broad range of healthcare markets. The company is headquartered in Louisville, Kentucky.

3. BrightSpring provides clinical care, support services, and pharmacy services to seniors and high-needs patients. It is headquartered in Louisville, Kentucky. BrightSpring is PharMerica's parent company.

4. Defendants collected and retain the PII/PHI of their patients, including Plaintiff and Class members, in connection with providing pharmacy services or other healthcare services or products. On March 14, 2023, Defendants learned that an unauthorized person or persons had accessed PharMerica's computer systems from March 12 to March 13, 2023, during which time the unauthorized person accessed and stole the sensitive PII/PHI of Plaintiff and Class members (the "Data Breach").

5. Defendants owed a duty to Plaintiff and Class members to implement and maintain reasonable and adequate security measures to secure, protect, and safeguard their PII/PHI against unauthorized access and disclosure. Defendants breached that duty by, among other things, failing to implement and maintain reasonable security procedures and practices to protect their customers' PII/PHI from unauthorized access and disclosure.

6. As a result of Defendants' inadequate security and breach of their duties and obligations, the Data Breach occurred, and Plaintiff's and Class members' PII/PHI was accessed and disclosed. This action seeks to remedy these failings and their consequences. Plaintiff brings this action on behalf of herself and all persons whose PII/PHI was exposed as a result of the Data Breach.

7. Plaintiff, on behalf of herself and all other Class members, asserts claims for negligence, breach of fiduciary duty, breach of implied contract, and unjust enrichment, and seeks declaratory relief, injunctive relief, monetary damages, statutory damages, punitive damages, equitable relief, and all other relief authorized by law.

PARTIES

Plaintiff Tandria Marallo

8. Plaintiff Tandria Marallo is a citizen of South Carolina.

9. Plaintiff receives pharmacy services from Defendants or affiliates of Defendants.

10. As a condition of receiving pharmacy services or other healthcare services or products, Defendants required Plaintiff Marallo to provide them with her PII/PHI.

11. Based on representations made by Defendants, Plaintiff believed Defendants had implemented and maintained reasonable security and practices to protect her PII/PHI. With this belief in mind, Plaintiff provided her PII/PHI to Defendants in connection with receiving pharmacy services or other healthcare services or products.

12. Defendants store and maintain Plaintiff's PII/PHI on their network systems.

13. Plaintiff takes great care to protect her PII/PHI. Had Plaintiff known that Defendants do not adequately protect the PII/PHI in their possession, she would not have obtained services from Defendants or agreed to provide them with her PII/PHI.

14. Plaintiff received notice through AT&T ActiveArmor alerting her that her information was affected by the Data Breach and posted on the dark web.

15. As a direct result of the Data Breach, Plaintiff Marallo has been the victim of identity theft: on or about May 7, 2023, Plaintiff had approximately $600 fraudulently charged to and removed from her bank account.

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

Defendant PharMerica Corporation

17. Defendant PharMerica Corporation is a Delaware corporation with its principal place of business in Louisville, Kentucky. PharMerica's headquarters are located at 805 N. Whittington Parkway, Louisville, Kentucky 40222. It may be served through its registered agent: Corporation Service Company, 421 West Main Street, Frankfort, KY 40601.

Defendant Res-Care, Inc., d/b/a BrightSpring Health Services

18. Defendant Res-Care, Inc., d/b/a BrightSpring Health Services is a Kentucky corporation with its headquarters in Louisville, Kentucky. BrightSpring's headquarters are located at 805 N. Whittington Parkway, Louisville, Kentucky 40222. It may be served through its registered agent: Corporation Service Company, 421 West Main Street, Frankfort, KY 40601.

JURISDICTION AND VENUE

19. The Court has subject matter jurisdiction over Plaintiff's claims under 28 U.S.C. § 1332(d)(2), because (a) there are 100 or more Class members, (b) at least one Class member is a citizen of a state that is diverse from Defendants, and (c) the matter in controversy exceeds $5,000,000, exclusive of interest and costs.

20. This Court has personal jurisdiction over PharMerica because PharMerica maintains its principal place of business in Kentucky and regularly transacts business in Kentucky.

21. This Court has personal jurisdiction over BrightSpring because BrightSpring is a Kentucky corporation, maintains its principal place of business in Kentucky, and regularly transacts business in Kentucky.

22. Venue is proper in this District pursuant to 28 U.S.C. § 1391(b)(2) because Defendants' principal places of business are in this District and a significant amount of the events leading to Plaintiff's causes of action occurred in this District.

FACTUAL ALLEGATIONS

Overview of PharMerica

23. "PharMerica is a national leader in pharmacy services," and serves "over 3,100 long-term care, senior living, IDD/behavioral health, home infusion, specialty pharmacy, and hospital management programs" in all 50 states.[1] It provides pharmacy services to "a broad array of healthcare markets, including long-term care, senior living, hospice, IDD/behavioral health, home infusion, specialty, and hospital management."[2]

24. PharMerica's website contains a Notice of Privacy Practices that describes how PharMerica's patients' medical information may be used.[3]

25. PharMerica acknowledges it is "required by law to: Maintain the privacy and security of your medical information, . . . Provide you with notice if a breach occurs that may have compromised the privacy or security of your medical information, [and] Abide by the terms of this Notice."[4]

26. PharMerica's Notice of Privacy Practices enumerates several ways that PharMerica will use and disclose its patients' information, including, *inter alia*, for treatment purposes, payment and billing, research, and to business associates.[5] The Notice explicitly states "[o]ther uses and disclosures of your medical information not covered by this Notice will be made only with [patients'] written authorization."[6] PharMerica acknowledges that "certain Federal and state

---

[1] *See Who We Are*, PHARMERICA, https://pharmerica.com/who-we-are/ (last accessed June 8, 2023).
[2] *Who We Serve*, PHARMERICA, https://pharmerica.com/who-we-serve/ (last accessed June 8, 2023).
[3] *Notice of Privacy Practices*, PHARMERICA, https://pharmerica.com/privacy-policy/ (last accessed June 8, 2023).
[4] *Id.*
[5] *Id.*
[6] *Id.*

laws may require special protections for certain medical information," and promises that "[i]f these laws do not permit disclosure of such information without obtaining your authorization, we will comply with those laws."[7]

27. PharMerica's Code of Business Conduct and Ethics ("Code of Ethics") states PharMerica will "comply with all federal, state and local laws, regulations and rules, including . . . federal and state patient privacy laws."[8] PharMerica requires all "[o]fficers, directors and employees and all other affected individuals [to] comply with," *inter alia*, "state privacy laws protect[ing] the privacy and security of individually identifiable health information."[9] PharMerica acknowledges that "Failure to comply with HIPAA and state privacy laws may subject. . . the Company to civil and criminal penalties."[10]

28. Plaintiff and Class members are, or were, customers of PharMerica or BrightSpring who entrusted PharMerica or BrightSpring with their PII/PHI.

Overview of BrightSpring

29. "BrightSpring Health Services is the leading provider of complementary home- and community-based health services for complex populations in need of specialized and/or chronic care."[11] It provides services including "home health care, hospice and home care to seniors, long-term specialty care to behavioral and neuro rehabilitation populations, and pharmacy therapy

[7] *Id.*
[8] *Code of Business Conduct and Ethics*, PHARMERICA, https://pharmerica.com/wp-content/uploads/2021/01/PharMerica-Code-of-Conduct-20201119.pdf (last accessed June 8, 2023).
[9] *Id.*
[10] *Id.*
[11] *About Us*, BRIGHTSPRING HEALTH SERVS., https://www.brightspringhealth.com/about-us/ (last accessed June 8, 2023).

management to patients across many settings."[12] It serves approximately 350,000 patients daily in all 50 states.[13]

30. BrightSpring claims its "processes and technology make us a leader in innovation with electronic health record solutions, signature programs, data analytics and reporting, smart home monitoring, telehealth, and clinical, behavioral and care management."[14]

31. BrightSpring's website contains a Notice of Privacy Practices.[15] BrightSpring states it "must follow the duties and privacy practices described in this notice."[16]

32. BrightSpring acknowledges it is "required by law to maintain the privacy and security of [patients'] protected health information."[17]

33. In the Notice of Privacy Practices, BrightSpring lists ways it can use patients' personal and health information, including, *inter alia*, to treat patients, bill patients, research, and to comply with the law.[18] It claims it "will not use or share [patients'] information other than as described" in the Notice of Privacy Practices unless a patient authorizes the disclosure in writing.[19]

34. BrightSpring promises to let patients "know promptly if a breach occurs that may have compromised the privacy or security of [their] information."[20]

---

[12] *Id.*
[13] *BrightSpring Fact Sheet*, BRIGHTSPRING HEALTH SERVS., https://www.brightspringhealth.com/wp-content/uploads/BHS-Fact-Sheet-04.22v4.pdf (last accessed June 8, 2023).
[14] *About Us*, *supra* note 11.
[15] *Notice of Privacy Practices*, BRIGHTSPRING HEALTH SERVS., https://www.brightspringhealth.com/wp-content/uploads/BrightSpring-PrivacyPractices.pdf (last accessed June 8, 2023).
[16] *Id.*
[17] *Id.*
[18] *Id.*
[19] *Id.*
[20] *Id.*

35. BrightSpring's Code of Conduct states "[a]ll information concerning persons supported by BrightSpring must be considered confidential and access limited to the person supported, guardian or legal representative, persons providing support or other persons specifically authorized."[21]

36. BrightSpring "collects information about a person's medical history, social history, treatment history and personal goals and abilities."[22] BrightSpring claims it "recognize[s] the sensitive nature of this information and [is] committed to maintaining confidentiality as required by local, state and federal regulations."[23]

37. BrightSpring requires "[a]ll programs and services [to] ensure that the privacy of the individuals we support is honored at all times. Without specific informed authorization, any . . . personal information may not be disclosed."[24]

38. Plaintiff and Class members are, or were, customers of PharMerica or BrightSpring who entrusted PharMerica or BrightSpring with their PII/PHI.

The Data Breach

39. According to a notice PharMerica posted on its website, "On March 14, 2023, PharMerica and its parent company, BrightSpring Health Services, Inc., learned of suspicious activity on their computer network."[25] Defendants determined "that an unknown third party accessed PharMerica computer systems from March 12-13, 2023, and that certain personal

---

[21] *Code of Conduct*, BRIGHTSPRING HEALTH SERVS., https://www.brightspringhealth.com/wp-content/uploads/BrightSpring-Code-of-Conduct-January-2022.pdf (last accessed June 8, 2023).
[22] *Id.*
[23] *Id.*
[24] *Id.*
[25] *PharMerica Notifies Individuals of Privacy Incident*, PHARMERICA, https://pharmerica.com/data-privacy-incident/ (last accessed June 8, 2023).

information may have been obtained as a part of the incident."[26]

40. Defendants "identified a data population whose personal information and limited medical information (names, dates of birth, Social Security numbers, medication lists and health insurance information) were disclosed."[27]

41. "Although PharMerica does not mention the type of hacking incident, the Money Message ransomware gang claimed the attack on March 28th, 2023, when they began publishing stolen data."[28] The Money Message ransomware gang

> was first observed targeting organizations worldwide and demanding million-dollar ransoms as early as mid-March. The group appears to routinely target large corporations that provide services to several subsidiaries impacting third-party entities and their customers. The group has published substantial quantities of victims' stolen data on their data leak site including . . . PharMerica.[29]

"This stolen data was published on the dark web leak site of the Money Message ransomware gang."[30] "The group claimed to have exfiltrated databases containing 4.7 terabytes of data."[31]

42. To prove the validity of the stolen data, "Money Message uploaded screencaps show[ing] part of a patient-related table with name, SSN, date of birth, Medicaid number, and Medicare number. There was also an Excel file with what appears to be protected health information

---

[26] *Id.*
[27] *Id.*
[28] Bill Toulas, *Ransomeware Gang Steals Data of 5.8 Million PharMerica Patients*, BleepingComputer (May 15, 2023, 2:10 PM), https://www.bleepingcomputer.com/news/security/ransomware-gang-steals-data-of-58-million-pharmerica-patients/.
[29] *Money Message Ransomware Targets NJ Organization*, N.J. CYBERSEC. & COMMC'N INTEGRATION CELL (May 25, 2023), https://www.cyber.nj.gov/alerts-advisories/money-message-ransomware-targets-nj-organization.
[30] Carly Page, *US Pharmacy Giant Says Hackers Accessed Personal Data of Almost 6 Million Patients*, TechCrunch (May 16, 2023, 8:15 AM), https://techcrunch.com/2023/05/16/us-pharmacy-giant-says-hackers-accessed-personal-data-of-almost-6-million-patients/.
[31] Steve Alder, *Almost 6 Million Individuals Affected by PharMerica Data Breach*, HIPAA J. (May 17, 2023), https://www.hipaajournal.com/almost-6-million-individuals-affected-by-pharmerica-data-breach/.

(PHI) on 100 patients, including name, date of birth, SSN, Medicaid Number, Medicare Number, allergies, and a field with somewhat detailed diagnoses information and history."[32]

43. On April 9, 2023, the Money Message ransomware gang "published what they claim is all of the stolen data on their extortion site."[33] A "threat actor has already posted the entire data dump on a . . . hacking forum, breaking the file into 13 parts for easier downloading."[34] The stolen PII/PHI was still available for download as of May 15, 2023.[35]

Defendants Knew that Criminals Target PII/PHI

44. At all relevant times, Defendants knew, or should have known, that the PII/PHI that they collected, shared, and stored was a target for malicious actors. Indeed, Defendants were both clearly aware of the threat of a data breach, as each promised to inform patients of the occurrence of a data breach.[36]

45. Defendants knew or should have known of these risks. Despite such knowledge, Defendants failed to implement and maintain reasonable and appropriate data privacy and security measures to protect Plaintiff's and Class members' PII/PHI from cyber-attacks that Defendants should have anticipated and guarded against.

46. It is well known amongst companies that store sensitive personally identifying information that sensitive information—such as the Social Security numbers ("SSNs") and medical information stolen in the Data Breach—is valuable and frequently targeted by criminals.

---

[32] *PharMerica and BrightSpring Health Services Hit by Money Message*, DATABREACHES.NET (Apr. 8, 2023), https://www.databreaches.net/pharmerica-and-brightspring-health-services-hit-by-money-message/.
[33] Toulas, *supra* note 28.
[34] *Id.*
[35] *Id.*
[36] *Notice of Privacy Practices*, *supra* note 4 (PharMerica); *Notice of Privacy Practices*, *supra* note 15 (BrightSpring).

In a recent article, *Business Insider* noted that "[d]ata breaches are on the rise for all kinds of businesses, including retailers . . . . Many of them were caused by flaws in . . . systems either online or in stores."[37]

47. Cyber criminals seek out PHI at a greater rate than other sources of personal information. In a 2023 report, the healthcare compliance company Protenus found that there were 956 medical data breaches in 2022 with over 59 million patient records exposed.[38] This is an increase from the 758 medical data breaches which exposed approximately 40 million records that Protenus compiled in 2020.[39]

48. PII/PHI is a valuable property right.[40] The value of PII/PHI as a commodity is measurable.[41] "Firms are now able to attain significant market valuations by employing business models predicated on the successful use of personal data within the existing legal and regulatory frameworks."[42] American companies are estimated to have spent over $19 billion on acquiring personal data of consumers in 2018.[43] It is so valuable to identity thieves that once PII/PHI has

---

[37] Dennis Green, Mary Hanbury & Aine Cain, *If you bought anything from these 19 companies recently, your data may have been stolen*, BUS. INSIDER (Nov. 19, 2019, 8:05 A.M.), https://www.businessinsider.com/data-breaches-retailers-consumer-companies-2019-1.
[38] *See* PROTENUS, *2023 Breach Barometer*, PROTENUS.COM, https://www.protenus.com/breach-barometer-report (last accessed June 8, 2023).
[39] *See id*.
[40] *See* Marc van Lieshout, *The Value of Personal Data*, 457 INT'L FED'N FOR INFO. PROCESSING 26 (May 2015) ("The value of [personal] information is well understood by marketers who try to collect as much data about personal conducts and preferences as possible…"), https://www.researchgate.net/publication/283668023_The_Value_of_Personal_Data.
[41] *See* Robert Lowes, *Stolen EHR [Electronic Health Record] Charts Sell for $50 Each on Black Market*, MEDSCAPE.COM (April 28, 2014), http://www.medscape.com/viewarticle/824192.
[42] OECD, *Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value*, OECD ILIBRARY (April 2, 2013), https://www.oecd-ilibrary.org/science-and-technology/exploring-the-economics-of-personal-data_5k486qtxldmq-en.
[43] *See* IAB Data Center of Excellence, *U.S. Firms to Spend Nearly $19.2 Billion on Third-Party Audience Data and Data-Use Solutions in 2018, Up 17.5% from 2017*, IAB.COM (Dec. 5, 2018), https://www.iab.com/news/2018-state-of-data-report/.

been disclosed, criminals often trade it on the "cyber black-market," or the "dark web," for many years.

49. As a result of the real and significant value of this material, identity thieves and other cyber criminals have openly posted credit card numbers, SSNs, PII/PHI, and other sensitive information directly on various Internet websites making the information publicly available. This information from various breaches, including the information exposed in the Data Breach, can be readily aggregated and become more valuable to thieves and more damaging to victims.

50. PHI is particularly valuable and has been referred to as a "treasure trove for criminals."[44] A cybercriminal who steals a person's PHI can end up with as many as "seven to ten personal identifying characteristics of an individual."[45]

51. All-inclusive health insurance dossiers containing sensitive health insurance information, names, addresses, telephone numbers, email addresses, SSNs, and bank account information, complete with account and routing numbers, can fetch up to $1,200 to $1,300 each on the black market.[46] According to a report released by the Federal Bureau of Investigation's ("FBI") Cyber Division, criminals can sell healthcare records for 50 times the price of a stolen Social Security or credit card number.[47]

---

[44] *See* Andrew Steager, *What Happens to Stolen Healthcare Data*, HEALTHTECH MAGAZINE (Oct. 20, 2019), https://healthtechmagazine.net/article/2019/10/what-happens-stolen-healthcare-data-perfcon ("*What Happens to Stolen Healthcare Data*") (quoting Tom Kellermann, Chief Cybersecurity Officer, Carbon Black, stating "Health information is a treasure trove for criminals.").

[45] *Id.*

[46] *See* SC Staff, *Health Insurance Credentials Fetch High Prices in the Online Black Market*, SC MAG. (July 16, 2013), https://www.scmagazine.com/news/breach/health-insurance-credentials-fetch-high-prices-in-the-online-black-market.

[47] *See* Federal Bureau of Investigation, *Health Care Systems and Medical Devices at Risk for Increased Cyber Intrusions for Financial Gain* (April 8, 2014), https://www.illuminweb.com/wp-content/uploads/ill-mo-uploads/103/2418/health-systems-cyber-intrusions.pdf.

52. Criminals can use stolen PII/PHI to extort a financial payment by "leveraging details specific to a disease or terminal illness."[48] Quoting Carbon Black's Chief Cybersecurity Officer, one recent article explained: "Traditional criminals understand the power of coercion and extortion . . . By having healthcare information—specifically, regarding a sexually transmitted disease or terminal illness—that information can be used to extort or coerce someone to do what you want them to do."[49]

53. Consumers place a high value on the privacy of that data, as they should. Researchers shed light on how much consumers value their data privacy—and the amount is considerable. Indeed, studies confirm that "when privacy information is made more salient and accessible, some consumers are willing to pay a premium to purchase from privacy protective websites."[50]

54. Given these facts, any company that transacts business with a consumer and then compromises the privacy of consumers' PII/PHI has thus deprived that consumer of the full monetary value of the consumer's transaction with the company.

Theft of PII/PHI Has Grave and Lasting Consequences for Victims

55. Theft of PII/PHI is serious. The FTC warns consumers that identity thieves use PII/PHI to exhaust financial accounts, receive medical treatment, start new utility accounts, and incur charges and credit in a person's name.[51]

---

[48] *What Happens to Stolen Healthcare Data*, *supra* note 44.
[49] *Id.*
[50] Janice Y. Tsai et al., *The Effect of Online Privacy Information on Purchasing Behavior*, *An Experimental Study*, 22(2) INFO. SYS. RSCH. 254 (June 2011) https://www.jstor.org/stable/23015560?seq=1.
[51] *See* Federal Trade Commission, *What to Know About Identity Theft*, FED. TRADE COMM'N CONSUMER INFO., https://www.consumer.ftc.gov/articles/what-know-about-identity-theft (last accessed June 8, 2023).

56. Identity thieves use personal information for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.[52] Experian, one of the largest credit reporting companies in the world, warns consumers that "[i]dentity thieves can profit off your personal information" by, among other things, selling the information, taking over accounts, using accounts without permission, applying for new accounts, obtaining medical procedures, filing a tax return, and applying for government benefits.[53]

57. With access to an individual's PII/PHI, criminals can do more than just empty a victim's bank account—they can also commit all manner of fraud, including: obtaining a driver's license or official identification card in the victim's name but with the thief's picture; using the victim's name and SSN to obtain government benefits; or, filing a fraudulent tax return using the victim's information. In addition, identity thieves may even give the victim's personal information to police during an arrest.[54]

---

[52] The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 12 C.F.R. § 1022.3(h). The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, social security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number." 12 C.F.R. § 1022.3(g).

[53] *See* Louis DeNicola, *What Can Identity Thieves Do with Your Personal Information and How Can You Protect Yourself*, EXPERIAN (May 21, 2023), https://www.experian.com/blogs/ask-experian/what-can-identity-thieves-do-with-your-personal-information-and-how-can-you-protect-yourself/.

[54] *See* Federal Trade Commission, *Warning Signs of Identity Theft*, IDENTITYTHEFT.GOV https://www.identitytheft.gov/Warning-Signs-of-Identity-Theft (last accessed June 8, 2023).

58. Identity theft is not an easy problem to solve. In a survey, the Identity Theft Resource Center found that most victims of identity crimes need more than a month to resolve issues stemming from identity theft and some need over a year.[55]

59. Theft of SSNs also creates a particularly alarming situation for victims because those numbers cannot easily be replaced. In order to obtain a new number, a breach victim has to demonstrate ongoing harm from misuse of their SSN, and a new SSN will not be provided until after the harm has already been suffered by the victim.

60. Due to the highly sensitive nature of SSNs, theft of SSNs in combination with other PII (e.g., name, address, date of birth) is akin to having a master key to the gates of fraudulent activity. TIME quotes data security researcher Tom Stickley, who is employed by companies to find flaws in their computer systems, as stating, "If I have your name and your Social Security number and you don't have a credit freeze yet, you're easy pickings."[56]

61. Theft of PII is even more serious when it includes theft of PHI. Data breaches involving medical information "typically leave[] a trail of falsified information in medical records that can plague victims' medical and financial lives for years."[57] It "is also more difficult to detect, taking almost twice as long as normal identity theft."[58] In warning consumers on the dangers of medical identity theft, the FTC states that an identity thief may use PII/PHI "to see a doctor, get

---

[55] *See* Identity Theft Resource Center, *2021 Consumer Aftermath Report*, IDENTITY THEFT RES. CTR. (2021), https://www.idtheftcenter.org/identity-theft-aftermath-study/ (last accessed June 8, 2022).

[56] Patrick Lucas Austin, *'It Is Absurd.' Data Breaches Show it's Time to Rethink How We Use Social Security Numbers, Experts Say*, TIME (August 5, 2019), https://time.com/5643643/capital-one-equifax-data-breach-social-security/.

[57] Pam Dixon and John Emerson, *The Geography of Medical Identity Theft*, FTC.GOV (Dec. 12, 2017), http://www.worldprivacyforum.org/wp-content/uploads/2017/12/WPF_Geography_of_Medical_Identity_Theft_fs.pdf.

[58] *See* Federal Bureau of Investigation, *Health Care Systems and Medical Devices at Risk…*, *supra* note 47.

prescription drugs, buy medical devices, submit claims with your insurance provider, or get other medical care." [59] The FTC also warns, "If the thief's health information is mixed with yours it could affect the medical care you're able to get or the health insurance benefits you're able to use."[60]

62. A report published by the World Privacy Forum and presented at the US FTC Workshop on Informational Injury describes what medical identity theft victims may experience:

- Changes to their health care records, most often the addition of falsified information, through improper billing activity or activity by imposters. These changes can affect the healthcare a person receives if the errors are not caught and corrected.
- Significant bills for medical goods and services neither sought nor received.
- Issues with insurance, co-pays, and insurance caps.
- Long-term credit problems based on problems with debt collectors reporting debt due to identity theft.
- Serious life consequences resulting from the crime; for example, victims have been falsely accused of being drug users based on falsified entries to their medical files; victims have had their children removed from them due to medical activities of the imposter; victims have been denied jobs due to incorrect information placed in their health files due to the crime.
- As a result of improper and/or fraudulent medical debt reporting, victims may not qualify for mortgage or other loans and may experience other financial impacts.
- Phantom medical debt collection based on medical billing or other identity information.
- Sales of medical debt arising from identity theft can perpetuate a victim's debt collection and credit problems, through no fault of their own.[61]

---

[59] *See What to Know About Medical Identity Theft*, FEDERAL TRADE COMMISSION CONSUMER INFORMATION, https://www.consumer.ftc.gov/articles/what-know-about-medical-identity-theft (last accessed June 8, 2023).
[60] *Id*.
[61] *See* Pam Dixon and John Emerson, *The Geography of Medical Identity Theft*, *supra* note 57.

63. There may also be a time lag between when sensitive personal information is stolen, when it is used, and when a person discovers it has been used. For example, on average it takes approximately three months for consumers to discover their identity has been stolen and used, but it takes some individuals up to three years to learn that information.[62]

64. It is within this context that Plaintiff and Class members must now live with the knowledge that their PII/PHI is forever in cyberspace and was taken by and in the possession of people willing to use the information for any number of improper purposes and scams, including making the information available for sale on the black-market.

Damages Sustained by Plaintiff and the Other Class Members

65. Plaintiff and Class members have suffered and will suffer injury, including, but not limited to: (i) a substantially increased and imminent risk of identity theft; (ii) the compromise, publication, and theft of their PII/PHI; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from unauthorized use of their PII/PHI; (iv) lost opportunity costs associated with efforts attempting to mitigate the actual and future consequences of the Data Breach; (v) the continued risk to their PII/PHI which remains in Defendants' possession; (vi) future costs in terms of time, effort, and money that will be required to prevent, detect, and repair the impact of the PII/PHI compromised as a result of the Data Breach; (vii) loss of value of the PII/PHI that was compromised in the Data Breach; and (viii) overpayment for the services that were received without adequate data security.

[62] John W. Coffey, *Difficulties in Determining Data Breach Impacts*, 17 J. OF SYSTEMICS, CYBERNETICS AND INFORMATICS 9 (2019), http://www.iiisci.org/journal/pdv/sci/pdfs/IP069LL19.pdf.

CLASS ALLEGATIONS

66. This action is brought and may be properly maintained as a class action pursuant to Rule 23 of the Federal Rules of Civil Procedure.

67. Plaintiff bring this action on behalf of herself and all members of the following Nationwide Class of similarly situated persons:

> All persons whose personally identifiable information or personal health information was compromised in the Data Breach by unauthorized persons, including all persons who were sent a notice of the Data Breach.

68. Excluded from the Class are PharMerica Corporation, and its affiliates, parents, subsidiaries, officers, agents, and directors; Res-Care, Inc., d/b/a BrightSpring Health Services, and its affiliates, parents, subsidiaries, officers, agents, and directors; as well as the judge(s) presiding over this matter and the clerks of said judge(s).

69. Certification of Plaintiff's claims for class-wide treatment is appropriate because Plaintiff can prove the elements of her 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.

70. The members in the Class are so numerous that joinder of each of the Class members in a single proceeding would be impracticable. PharMerica reported to the U.S. Department of Health and Human Services that approximately 5,815,591 persons' information was exposed in the Data Breach.[63]

71. Common questions of law and fact exist as to all Class members and predominate over any potential questions affecting only individual Class members. Such common questions of law or fact include, *inter alia*:

a. Whether Defendants had a duty to implement and maintain reasonable security

[63] *See Breach Portal*, U.S. DEP'T OF HEALTH AND HUMAN SERVS., https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (last accessed June 8, 2023).

procedures and practices to protect and secure Plaintiff's and Class members' PII/PHI from unauthorized access and disclosure;

b. Whether Defendants had duties not to disclose the PII/PHI of Plaintiff and Class members to unauthorized third parties;

c. Whether Defendants failed to exercise reasonable care to secure and safeguard Plaintiff's and Class members' PII/PHI;

d. Whether an implied contract existed between Class members and Defendants, providing that Defendants would implement and maintain reasonable security measures to protect and secure Class members' PII/PHI from unauthorized access and disclosure;

e. Whether Defendants engaged in unfair, unlawful, or deceptive practices by failing to safeguard the PII/PHI of Plaintiff and Class members;

f. Whether Defendants breached their duties to protect Plaintiff's and Class members' PII/PHI; and

g. Whether Plaintiff and Class members are entitled to damages, and the measure of such damages and relief.

72. Defendants engaged in a common course of conduct giving rise to the legal rights sought to be enforced by Plaintiff, on behalf of herself and all other Class members. Individual questions, if any, pale in comparison, in both quantity and quality, to the numerous common questions that dominate this action.

73. Plaintiff's claims are typical of the claims of the Class. Plaintiff, like all proposed members of the Class, had her PII/PHI compromised in the Data Breach. Plaintiff and Class members were injured by the same wrongful acts, practices, and omissions committed by Defendants, as described herein. Plaintiff's claims therefore arise from the same practices or course of conduct that give rise to the claims of all Class members.

74. Plaintiff will fairly and adequately protect the interests of the Class members. Plaintiff is an adequate representative of the Class in that she has no interests adverse to, or that conflict with, the Class she seeks to represent. Plaintiff has retained counsel with substantial

experience and success in the prosecution of complex consumer protection class actions of this nature.

75. 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 and other financial detriment suffered by Plaintiff and Class members are relatively small compared to the burden and expense that would be required to individually litigate their claims against Defendants, so it would be impracticable for Class members to individually seek redress from Defendants' 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, economy of scale, and comprehensive supervision by a single court.

CAUSES OF ACTION

COUNT I
NEGLIGENCE

76. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

77. Defendants owed a duty to Plaintiff and Class members to exercise reasonable care in safeguarding, securing, and protecting the PII/PHI in their possession, custody, or control.

78. Defendants knew or should have known the risks of collecting and storing Plaintiff's and all other Class members' PII/PHI and the importance of maintaining and using secure systems. Defendants knew or should have known of the many data breaches that have targeted companies that stored PII/PHI in recent years.

79. Given the nature of Defendants' businesses, the sensitivity and value of the PII/PHI they maintain, and the resources at their disposal, Defendants should have identified and foreseen the vulnerabilities in their systems and prevented the dissemination of Plaintiff's and Class members' PII/PHI.

80. Defendants makes explicit statements on their websites that they are aware of the risk of potential data breaches, that they will follow privacy laws and regulations, and that they will use reasonable methods to protect the PII/PHI in their possession.

81. Defendants breached these duties by failing to exercise reasonable care in safeguarding and protecting Plaintiff's and Class members' PII/PHI by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems to safeguard and protect PII/PHI entrusted to them—including Plaintiff's and Class members' PII/PHI.

82. Plaintiff and Class members had no ability to protect their PII/PHI that was, or remains, in Defendants' possession.

83. It was or should have been reasonably foreseeable to Defendants that their failure to exercise reasonable care in safeguarding and protecting Plaintiff's and Class members' PII/PHI by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems would result in the unauthorized release, disclosure, and dissemination of Plaintiff's and Class members' PII/PHI to unauthorized individuals.

84. But for Defendants' negligent conduct or breach of the above-described duties owed to Plaintiff and Class members, their PII/PHI would not have been compromised. The

PII/PHI of Plaintiff and the Class was accessed and stolen as the proximate result of Defendants' failure to exercise reasonable care in safeguarding, securing, and protecting such PII/PHI by, *inter alia*, adopting, implementing, and maintaining appropriate security measures.

85. As a result of Defendants' above-described wrongful actions, inaction, and want of ordinary care that directly and proximately caused the Data Breach, Plaintiff and Class members have suffered and will suffer injury, including, but not limited to: (i) a substantially increased and imminent risk of identity theft; (ii) the compromise, publication, and theft of their PII/PHI; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from unauthorized use of their PII/PHI; (iv) lost opportunity costs associated with efforts attempting to mitigate the actual and future consequences of the Data Breach; (v) the continued risk to their PII/PHI which remains in Defendants' possession; (vi) future costs in terms of time, effort, and money that will be required to prevent, detect, and repair the impact of the PII/PHI compromised as a result of the Data Breach; (vii) loss of value of the PII/PHI that was compromised in the Data Breach; and (viii) overpayment for the services that were received without adequate data security.

COUNT II
BREACH OF FIDUCIARY DUTY

86. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

87. As a condition of obtaining services or employment from Defendants, Plaintiff and Class members gave Defendants their PII/PHI in confidence, believing that Defendants would protect that information. Plaintiff and Class members would not have provided Defendants with this information had they known it would not be adequately protected. Defendants' acceptance and storage of Plaintiff's and Class members' PII/PHI created a fiduciary relationship between Defendants and Plaintiff and Class members. In light of this

relationship, Defendants must act primarily for the benefit of their customers, which includes safeguarding and protecting Plaintiff's and Class Members' PII/PHI.

88. Defendants have a fiduciary duty to act for the benefit of Plaintiff and Class members upon matters within the scope of their relationship. They breached that duty by failing to ensure that the third-parties they contract with and share PII/PHI with properly protect the integrity of the system containing Plaintiff's and Class members' PII/PHI, failing to comply with the data security guidelines set forth by HIPAA, and otherwise failing to safeguard Plaintiff's and Class members' PII/PHI that they collected, shared, and stored.

89. As a direct and proximate result of Defendants' breach of their fiduciary duties, Plaintiff and Class members have suffered and will suffer injury, including, but not limited to: (i) a substantially increased and imminent risk of identity theft; (ii) the compromise, publication, and theft of their PII/PHI; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from unauthorized use of their PII/PHI; (iv) lost opportunity costs associated with efforts attempting to mitigate the actual and future consequences of the Data Breach; (v) the continued risk to their PII/PHI which remains in Defendants' possession; (vi) future costs in terms of time, effort, and money that will be required to prevent, detect, and repair the impact of the PII/PHI compromised as a result of the Data Breach; (vii) loss of value of the PII/PHI that was compromised in the Data Breach; and (viii) overpayment for the services that were received without adequate data security.

COUNT III
BREACH OF IMPLIED CONTRACT

90. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

91. In connection with receiving pharmacy services or other healthcare services or products, Plaintiff and all other Class members entered into implied contracts with Defendants.

92. Pursuant to these implied contracts, Plaintiff and Class members benefited Defendants by paying monies to Defendants, directly or through their insurance, and provided Defendants with their PII/PHI. In exchange, Defendants agreed to, among other things, and Plaintiff understood that Defendants would: (1) provide pharmacy services or other healthcare services or products to Plaintiff and Class members; (2) take reasonable measures to protect the security and confidentiality of Plaintiff's and Class members' PII/PHI; (3) protect Plaintiff's and Class members' PII/PHI in compliance with federal and state laws and regulations and industry standards; and (4) maintain reasonable measures to protect the security and confidentiality of Plaintiff's and Class members' PII/PHI.

93. The protection of PII/PHI was a material term of the implied contracts between Plaintiff and Class members, on the one hand, and Defendants, on the other hand. Indeed, as set forth *supra*, Defendants recognized the importance of data security and the privacy of their customers' PII/PHI. Had Plaintiff and Class members known that Defendants would not adequately protect their PII/PHI, they would not have paid for products or services from Defendants.

94. Plaintiff and Class members performed their obligations under the implied contract when they provided Defendants with their PII/PHI and paid monies for products and services from Defendants, expecting that their PII/PHI would be protected.

95. Defendants breached their obligations under their implied contracts with Plaintiff and Class members by failing to implement and maintain reasonable security

measures to protect and secure their PII/PHI, and in failing to ensure that they third-parties they contract with and share PII/PHI with implement and maintain security protocols and procedures to protect Plaintiff's and Class members' PII/PHI in a manner that complies with applicable laws, regulations, and industry standards.

96. Defendants' breach of their obligations of the implied contracts with Plaintiff and Class members directly resulted in the Data Breach and the resulting injuries to Plaintiff and Class members.

97. Plaintiff and all other Class members were damaged by Defendants' breach of implied contracts because: (i) they paid monies (directly or indirectly) to Defendants in exchange for data security protection they did not receive; (ii) they now face a substantially increased and imminent risk of identity theft and medical identity theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (iii) their PII/PHI was improperly disclosed to unauthorized individuals; (iv) the confidentiality of their PII/PHI has been breached; (v) they were deprived of the value of their PII/PHI, for which there is a well-established national and international market; (vi) they lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of medical identity theft they face and will continue to face; and (vii) they overpaid for the services that were received without adequate data security.

COUNT IV
UNJUST ENRICHMENT

98. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

99. This claim is pleaded in the alternative to the breach of implied contract claim.

100. In obtaining services from Defendants, Plaintiff and Class members provided and entrusted their PII and PHI to Defendants.

101. Plaintiff and Class members conferred a monetary benefit upon Defendants in the form of monies paid for pharmacy services or other healthcare services or products with an implicit understanding that Defendants would use some of their revenue to protect the PII/PHI they collect and store.

102. Defendants accepted or had knowledge of the benefits conferred upon them by Plaintiff and Class Members. Defendants benefitted from the receipt of Plaintiff's and Class members' PII/PHI, as this was used to facilitate billing and payment services, which enabled Defendants to carry out their business.

103. As a result of Defendants' conduct, Plaintiff and Class members suffered actual damages in an amount equal to the difference in value between their payments made with reasonable data privacy and security practices and procedures that Plaintiff and Class members paid for and expected, and those payments without reasonable data privacy and security practices and procedures that they received.

104. Defendants should not be permitted to retain the money belonging to Plaintiff and Class members because Defendants failed to adequately implement the data privacy and security procedures for themselves and the third parties that they contract with and share PII/PHI with that Plaintiff and Class members paid for and expected, and that were otherwise mandated by federal, state, and local laws and industry standards.

105. Defendants should be compelled to provide for the benefit of Plaintiff and Class members all unlawful proceeds they received as a result of the conduct and Data Breach alleged herein.

PRAYER FOR RELIEF

Plaintiff, individually and on behalf of all other members of the Class, respectfully request that the Court enter judgment in their favor and against Defendants as follows:

A. Certifying the Class as requested herein, designating Plaintiff as Class representative, and appointing Plaintiff's counsel as Class Counsel;

B. Awarding Plaintiff and the Class appropriate monetary relief, including actual damages, statutory damages, punitive damages, restitution, and disgorgement;

C. Awarding Plaintiff and the Class equitable, injunctive, and declaratory relief, as may be appropriate. Plaintiff, on behalf of herself and the Class, seeks appropriate injunctive relief designed to prevent Defendants from experiencing another data breach by adopting and implementing best data security practices to safeguard PII/PHI and to provide or extend credit monitoring services and similar services to protect against all types of identity theft and medical identity theft;

D. Awarding Plaintiff and the Class pre-judgment and post-judgment interest to the maximum extent allowable;

E. Awarding Plaintiff and the Class reasonable attorneys' fees, costs, and expenses, as allowable; and

F. Awarding Plaintiff and the Class such other favorable relief as allowable under law.

JURY TRIAL DEMANDED

Plaintiff demands a trial by jury of all claims in this Class Action Complaint so triable.

Dated: June 9, 2023

Respectfully submitted,

/s/ Matthew L. White

Matthew L. White (#88595)
Mark K. Gray (#83552)
Gray & White Law
2301 River Road Suite 300
Louisville, KY 40206
Tel: 502-210-8942
Fax: 502-618-4059
mwhite@grayandwhitelaw.com
mgray@grayandwhitelaw.com

Ben Barnow*
Anthony L. Parkhill*
Barnow and Associates, P.C.
205 West Randolph Street, Ste. 1630
Chicago, IL 60606
Tel: 312-621-2000
Fax: 312-641-5504
b.barnow@barnowlaw.com
aparkhill@barnowlaw.com

Counsel for Plaintiff

* *Pro hac vice forthcoming*

ClassAction.org

This complaint is part of ClassAction.org's searchable class action lawsuit database and can be found in this post: PharMerica, BrightSpring Hit with Class Action Over March 2023 Cyberattack Affecting 5.8M
