UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF KENTUCKY
LOUISVILLE DIVISION

JAKETRIUS LURRY, on behalf of herself and all others similarly situated, Plaintiff, v. PHARMERICA CORPORATION, Defendant.	Case No. 3:23CV-297-RGJ **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Jaketrius Lurry ("Plaintiff") brings this Class Action Complaint on behalf of herself, and all others similarly situated, against Defendant PharMerica Corporation ("PharMerica" or "Defendant"), alleging as follows based upon information and belief and investigation of counsel, except as to the allegations specifically pertaining to her, which are based on personal knowledge:

NATURE OF THE ACTION

1. Healthcare providers that handle sensitive, personally identifying information ("PII") or protected health information ("PHI") owe a duty to the individuals to whom that data relates. This duty arises because it is foreseeable that the exposure of PII or PHI to unauthorized persons—and especially hackers with nefarious intentions—will result in harm to the affected individuals, including, but not limited to, the invasion of their private health matters.

2. The harm resulting from a data and privacy breach manifests in a number of ways, including identity theft and financial fraud, and the exposure of a person's PII or PHI through a data breach ensures that such person will be at a substantially increased and certainly impending risk of identity theft crimes compared to the rest of the population, potentially for the rest of their

lives. Mitigating that risk—to the extent it is even possible to do so—requires individuals to devote significant time and money to closely monitor their credit, financial accounts, health records, and email accounts, and take a number of additional prophylactic measures.

3. Defendant PharMerica is a national pharmacy that services patients of more than 3,100 long-term care, senior living, behavior health, home infusion, specialty pharmacy, and hospital management programs.[1] In total, PharMerica operates 180 pharmacies located in all 50 states.[2]

4. As a healthcare provider, Defendant knowingly collects and stores a litany of highly sensitive PII and PHI from its patients. In turn, PharMerica has a resulting duty to secure, maintain, protect, and safeguard the PII and PHI that it collects and stores against unauthorized access and disclosure through reasonable and adequate data security measures.

5. PharMerica expressly recognizes its duty to securely maintain its patients' PII and PHI in confidence. Defendant's Notice of Privacy Practices informs patients that PharMerica is "committed to protecting privacy of [patients'] medical information."[3]

6. Despite PharMerica's duty to safeguard its patients' PII and PHI, Plaintiff's and Class Members' PII and PHI was accessed and exfiltrated by an unknown third party who gained access to Defendant's computer systems between March 12 and 13, 2023 (the "Data Breach").[4]

7. Based on the public statements of PharMerica to date, a wide variety of PII and PHI were implicated in the Data Breach, including, but not limited to personal and medical information

---

[1] *Who We* Are, PharMerica, https://pharmerica.com/who-we-are/ (last visited June 6, 2023).
[2] *Id.*
[3] *Notice of Privacy Practices*, PharMerica (Oct. 28, 2019), https://pharmerica.com/privacy-policy/#:~:text=You%20have%20the%20right%20to%20ask%20us%20not%20to%20use,writing%20to%20our%20Privacy%20Officer.
[4] *PharMerica Notifies Individuals of Privacy Incident*, PharMerica, https://pharmerica.com/data-privacy-incident/ (last visited June 6, 2023) ("Notice of Data Breach").

such as names, dates of birth, Social Security numbers, medication lists, and health insurance information.

8. As a direct and proximate result of Defendant's inadequate data security measures, and its breach of its duty to handle patient PII and PHI with reasonable care, Plaintiff's and Class Members' PII and PHI have been accessed by hackers and exposed to an untold number of unauthorized individuals.

9. Plaintiff and Class Members are now at a significantly increased and certainly impending risk of fraud, identity theft, misappropriation of health insurance benefits, intrusion of their health privacy, and similar forms of criminal mischief, risk which may last for the rest of their lives. Consequently, Plaintiff and Class Members must devote substantially more time, money, and energy to protect themselves, to the extent possible, from these crimes.

10. Plaintiff, on behalf of herself, and the Class as defined herein, brings claim for negligence, negligence *per se*, breach of an implied contract, unjust enrichment, and declaratory judgment, seeking actual and putative damages, with attorneys' fees, costs, and expenses, and appropriate injunctive and declaratory relief.

PARTIES

11. Jaketrius Lurry is an adult, who at all relevant times, is and was a resident and citizen of the State of Georgia. Plaintiff was a patient of Defendant. Plaintiff received a Data Breach notice from PharMerica informing her that her PII and PHI that she entrusted to Defendant was compromised in the Data Breach.

12. Since the announcement of the Data Breach, Plaintiff has suffered actual identity theft noticing suspicious medical charges to her medical account even though they were not billed in her name. As a result of the Data Breach, Plaintiff has been required to spend her valuable time monitoring her financial and medical accounts and changing her passwords to the same to detect

and prevent any additional misuses of her PII and PHI. Plaintiff would not have to undergo such time-consuming efforts but for the Data Breach.

13. Since the announcement of the Data Breach Plaintiff has also received a significant increase in spam calls and texts as compared to prior to the Data Breach. Plaintiff has further suffered emotional distress as a result of her PII and PHI being accessed and exposed to an unauthorized third-party.

14. As a result of the Data Breach, Plaintiff will continue to be at heightened and certainly impending risk for fraud and identity theft, and their attendant damages for years to come.

15. Defendant PharMerica is a Delaware corporation with a principal place of business located at 805 N. Whittington Parkway, Louisville, Kentucky 40222. Defendant is a citizen of Delaware and Kentucky.

JURISDICTION AND VENUE

16. This Court has subject matter jurisdiction pursuant to 28 U.S.C. § 1332(d)(2)(A) because this case is a class action where the aggregate claims of all members of the proposed class are in excess of $5,000,000.00, exclusive of interest and costs, there are 100 or more members of the proposed class, and at least one member of the proposed class is a citizen of a state different than Defendant.

17. This Court has personal jurisdiction over Defendant because a substantial part of the events, omissions, and acts giving rise to the claims herein occurred in this District and Defendant resides in this District.

18. Venue is proper in this Court pursuant to 28 U.S.C. § 1391 because a substantial part of the events, omissions, and acts giving rise to the claims herein occurred in this District and Defendant resides in this District.

FACTUAL BACKGROUND

A. PharMerica Collected and Stored Plaintiff's and Class Members PII and PHI.

19. PharMerica is a full-service pharmacy, billing itself as "a national leader in pharmacy services, serving our partners in over 3,100 long-term care, senior living, IDD/behavioral health, home infusion, specialty pharmacy, and hospital management programs."[5]

20. As a condition of providing its medication services to Plaintiff and Class Members, PharMerica receives, creates, and handles PII and PHI, which includes, *inter alia*, patients' names, dates of birth, Social Security numbers, medication lists, and health insurance information.

21. Plaintiff and Class Members directly or indirectly entrusted PharMerica with their sensitive and confidential PII and PHI and therefore reasonably expected that Defendant would safeguard their highly sensitive PII and PHI and keep it confidential.

22. By obtaining, collecting, and storing Plaintiff's and Class Members' PII and PHI, PharMerica assumed equitable and legal duties to safeguard and keep confidential Plaintiff's and Class Members' highly sensitive information, to only use this information for business purposes, and to only make authorized disclosures.

23. Despite these duties, PharMerica failed to implement reasonable data security measures to protect Plaintiff's and Class Members' PII and PHI, and ultimately allowed nefarious third-party hackers to breach its computer systems, compromising Plaintiff's and Class Members' PII and PHI stored therein.

B. PharMerica Knew the Risks of Storing Valuable PII and PHI and the Foreseeable Harm to Victims.

24. PharMerica was well aware that the PHI and PII it collects is highly sensitive and of significant value to those who would use it for wrongful purposes.

[5] *Who We* Are, PharMerica, https://pharmerica.com/who-we-are/ (last visited June 6, 2023).

25. PharMerica also knew that a breach of its computer systems, and exposure of the information stored therein, would result in the increased risk of identity theft and fraud against the individuals whose PII and PHI was compromised, as well as intrusion into their highly private health information.

26. These risks are not theoretical; in recent years, numerous high-profile breaches have occurred at business such as Equifax, Facebook, Yahoo, Marriott, Anthem, and many others.

27. PII has considerable value and constitutes an enticing and well-known target to hackers. Hackers easily can sell stolen data as there has been a "proliferation of open and anonymous cybercrime forums on the Dark Web that serve as a bustling marketplace for such commerce."[6] PHI, in addition to being of a highly personal and private nature, can be used for medical fraud and to submit false medical claims for reimbursement.

28. The prevalence of data breaches and identity theft has increased dramatically in recent years, accompanied by a parallel and growing economic drain on individuals, businesses, and government entities in the U.S. In 2021, there were 4,145 publicly disclosed data breaches, exposing 22 billion records. The United States specifically saw a 10% increase in the total number of data breaches.[7]

29. In tandem with the increase in data breaches, the rate of identity theft complaints has also increased over the past few years. For instance, in 2017, 2.9 million people reported some form of identity fraud compared to 5.7 million people in 2021.[8]

---

[6] Brian Krebs, *The Value of a Hacked Company*, Krebs on Security (July 14, 2016), http://krebsonsecurity.com/2016/07/the-value-of-a-hacked-company/.

[7] *Data Breach Report: 2021 Year End*, Risk Based Security (Feb. 4, 2022), https://www.riskbasedsecurity.com/2022/02/04/data-breach-report-2021-year-end/.

[8] *Insurance Information Institute, Facts + Statistics: Identity theft and cybercrime*, Insurance Information Institute, https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-

30. The healthcare industry has become a prime target for threat actors: "High demand for patient information and often-outdated systems are among the nine reasons healthcare is now the biggest target for online attacks."[9] Indeed, "[t]he IT environments of healthcare organizations are often complex and difficult to secure. Devices and software continue to be used that have reached end-of-life, as upgrading is costly and often problematic. Many healthcare providers use software solutions that have been developed to work on specific – and now obsolete – operating systems and cannot be transferred to supported operating systems."[10]

31. Additionally, "[h]ospitals store an incredible amount of patient data. Confidential data that's worth a lot of money to hackers who can sell it on easily – making the industry a growing target."[11]

32. Cybercriminals seek out PHI at a greater rate than other sources of personal information. Between 2009 and 2022, 5,150 healthcare data breaches of 500 or more individuals have been reported to Health and Human Services' Office of Civil Rights, resulting in the exposure or unauthorized disclosure of the information of 382,262,109 individuals—"[t]hat equates to more than 1.2x the population of the United States."[12]

33. Further, the rate of healthcare data breaches has been on the rise in recent years. "In 2018, healthcare data breaches of 500 or more records were being reported at a rate of around 1

---

cybercrime#Identity%20Theft%20And%20Fraud%20Reports,%202015-2019%20 (last visited June 6, 2023).

[9] *The healthcare industry is at risk*, SwivelSecure https://swivelsecure.com/solutions/healthcare/healthcare-is-the-biggest-target-for-cyberattacks/ (last visited June 6, 2023).

[10] Steve Alder, Editorial: *Why Do Criminals Target Medical Records*, HIPAA Journal (Oct. 14, 2022), https://www.hipaajournal.com/why-do-criminals-target-medical-records/#:~:text=Healthcare%20records%20are%20so%20valuable,credit%20cards%20in %20victims'%20names.

[11] *Id.*

[12] *Healthcare Data Breach Statistics*, HIPAA Journal, https://www.hipaajournal.com/healthcare-data-breach-statistics/ (last visited June 6, 2023).

per day. Fast forward 5 years and the rate has more than doubled. In 2022, an average of 1.94 healthcare data breaches of 500 or more records were reported each day."[13]

34. In a 2022 report, the healthcare compliance company Protenus found that there were 905 medical data breaches in 2021, leaving over 50 million patient records exposed for 700 of the 2021 incidents. This is an increase from the 758 medical data breaches that Protenus compiled in 2020.[14]

35. The healthcare sector suffered about 337 breaches in the first half of 2022 alone, according to Fortified Health Security's mid-year report released in July. The percentage of healthcare breaches attributed to malicious activity rose more than 5 percentage points in the first six months of 2022 to account for nearly 80 percent of all reported incidents.[15]

36. The breadth of data compromised in the Data Breach makes the information particularly valuable to thieves and leaves PharMerica's patients especially vulnerable to identity theft, tax fraud, medical fraud, credit and bank fraud, and more.

37. **Social Security numbers**—Unlike credit or debit card numbers in a payment card data breach—which can quickly be frozen and reissued in the aftermath of a breach—unique social security numbers cannot be easily replaced. Even when such numbers are replaced, the process of doing so results in a major inconvenience to the subject person, requiring a wholesale review of the person's relationships with government agencies and any number of private companies in order to update the person's accounts with those entities.

---

[13] *Id.*

[14] *2022 Breach Barometer*, PROTENUS, https://www.protenus.com/breach-barometer-report (last visited June 6, 2023).

[15] Jill McKeon, *Health Sector Suffered 337 Healthcare Data Breaches in First Half of Year*, Cybersecurity News (July 19, 2022), https://healthitsecurity.com/news/health-sector-suffered-337-healthcare-data-breaches-in-first-half-of-year.

38. The Social Security Administration even warns that the process of replacing a Social Security is a difficult one that creates other types of problems, and that it will not be a panacea for the affected person:

> Keep in mind that a new number probably will not solve all your problems. This is because other governmental agencies (such as the IRS and state motor vehicle agencies) and private businesses (such as banks and credit reporting companies) likely will have records under your old number. Along with other personal information, credit reporting companies use the number to identify your credit record. So using a new number will not guarantee you a fresh start. This is especially true if your other personal information, such as your name and address, remains the same.
>
> If you receive a new Social Security Number, you should not be able to use the old number anymore.
>
> For some victims of identity theft, a new number actually creates new problems. If the old credit information is not associated with your new number, the absence of any credit history under the new number may make more difficult for you to get credit.[16]

39. Social security numbers allow individuals to apply for credit cards, student loans, mortgages, and other lines of credit—among other services. Often social security numbers can be used to obtain medical goods or services, including prescriptions. They are also used to apply for a host of government benefits. Access to such a wide range of assets makes social security numbers a prime target for cybercriminals and a particularly attractive form of PII to steal and then sell.

40. **Healthcare Records**—As indicated by Jim Trainor, former second in command at the FBI's cyber security division: "Medical records are a gold mine for criminals—they can access a patient's name, DOB, Social Security and insurance numbers, and even financial information all in one place. Credit cards can be, say, five dollars or more where PHI records can go from $20 say

[16] *Identify Theft and Your Social Security Numbers*, Social Security Admin. (June 2021), https://www.ssa.gov/pubs/EN-05-10064.pdf.

up to—we've even seen $60 or $70."[17] A complete identity theft kit that includes health insurance credentials may be worth up to $1,000 on the black market, whereas stolen payment card information sells for about $1.[18]

41. Indeed, medical records "are so valuable because they can be used to commit a multitude of crimes. Healthcare data can be used to impersonate patients to obtain expensive medical services, Medicare and Medicaid benefits, healthcare devices, and prescription medications. Healthcare records also contain the necessary information to allow fraudulent tax returns to be filed to obtain rebates."[19]

42. "In contrast to credit card numbers and other financial information, healthcare data has an incredibly long lifespan and can often be misused for long periods undetected. Credit card companies monitor for fraud and rapidly block cards and accounts if suspicious activity is detected, but misuse of healthcare data is harder to identify and can be misused in many ways before any malicious activity is detected. During that time, criminals can run up huge debts – far more than is usually possible with stolen credit card information."[20]

43. According to Experian:

> Having your records stolen in a healthcare data breach can be a prescription for financial disaster. If scam artists break into healthcare networks and grab your medical information, they can impersonate you to get medical services, use your data open credit accounts, break into your bank accounts, obtain drugs illegally, and even blackmail you with sensitive personal details.

---

[17] *You Got It, They Want It: Criminals Targeting Your Private Healthcare Data*, *New Ponemon Study Shows*, IDX (May 14, 2015), https://www.idexpertscorp.com/knowledge-center/single/you-got-it-they-want-it-criminals-are-targeting-your-private-healthcare-dat.

[18] *Managing cyber risks in an interconnected world, Key findings from The Global State of Information Security® Survey 2015*, PriceWaterhouseCoopers, https://www.pwc.com/gx/en/consulting-services/information-security-survey/assets/the-global-state-of-information-security-survey-2015.pdf (last visited June 6, 2023).

[19] Alder, *supra* note 10.

[20] *Id.*

> ID theft victims often have to spend money to fix problems related to having their data stolen, which averages $600 according to the FTC. But security research firm Ponemon Institute found that healthcare identity theft victims spend nearly $13,500 dealing with their hassles, which can include the cost of paying off fraudulent medical bills.
>
> Victims of healthcare data breaches may also find themselves being denied care, coverage or reimbursement by their medical insurers, having their policies canceled or having to pay to reinstate their insurance, along with suffering damage to their credit ratings and scores. In the worst cases, they've been threatened with losing custody of their children, been charged with drug trafficking, found it hard to get hired for a job, or even been fired by their employers.[21]

44. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches: "[I]n some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the [Dark] Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm."[22]

45. **Health Insurance Information** – "stolen personal health insurance information can be used by criminals to obtain expensive medical services, devices and prescription medications, as well as to fraudulently acquire government benefits like Medicare or Medicaid."[23]

46. Even if stolen PII or PHI does not include financial or payment card account information, that does not mean there has been no harm, or that the breach does not cause a substantial risk of identity theft. Freshly stolen information can be used with success against

---

[21] Brian O'Connor, *Healthcare Data Breach: What to Know About them and What to Do After One*, EXPERIAN (June 14, 2018), https://www.experian.com/blogs/ask-experian/healthcare-data-breach-what-to-know-about-them-and-what-to-do-after-one/.

[22] U.S. Gov't Accountability Office, Report to Congressional Requesters, Personal Information, June 2007: https://www.gao.gov/new.items/d07737.pdf (last visited June 6, 2023).

[23] Kate O'Flaherty, Why cyber-Criminals Are Attacking Healthcare - - And How to Stop Them, Forbes (Oct. 5, 2018), https://www.forbes.com/sites/kateoflahertyuk/2018/10/05/why-cyber-criminals-are-attacking-healthcare-and-how-to-stop-them/?sh=54e8ed1e7f69.

victims in specifically targeted efforts to commit identity theft known as social engineering or spear phishing. In these forms of attack, the criminal uses the previously obtained PII and PHI about the individual, such as name, address, email address, and affiliations, to gain trust and increase the likelihood that a victim will be deceived into providing the criminal with additional information.

47. Based on the value of its patients' PII and PHI to cybercriminals, PharMerica knew or should have known, the importance of safeguarding the PII and PHI entrusted to it and of the foreseeable consequences if its data security systems were breached. PharMerica failed, however, to take adequate cyber security measures to prevent the Data Breach from occurring.

C. PharMerica Breached its Duty to Protect its Patients' PII and PHI.

48. On or about April 8, 2023, reports of a data breach at PharMerica began to surface after the Money Message ransomware group added PharMerica to its list of victims.[24]

49. Money Message is a new ransomware operation that launch around March 2023 and gained attention for its ransomware attack on a Taiwanese PC parts maker, Micro-Star International.[25]

50. Specifically, Money Message claimed to have stolen 4.7 TB of data during their ransomware attack on PharMerica, including the personal information of two million individuals.[26]

---

[24] Dissent, *PharMerica and BrightSpring Health Services hit by Money Message*, DataBreaches.net (last updated Apr. 14, 2023), https://www.databreaches.net/pharmerica-and-brightspring-health-services-hit-by-money-message/.

[25] Bill Toulas, *New Money Message ransomware demands million dollar ransoms*, BleepingComputer (Apr. 2, 2023), https://www.bleepingcomputer.com/news/security/new-money-message-ransomware-demands-million-dollar-ransoms/; Bill Toulas, *Money Message ransomware gang claims MSI breach, demands $4 million*, BleepingComputer (Apr. 6, 2023), https://www.bleepingcomputer.com/news/security/money-message-ransomware-gang-claims-msi-breach-demands-4-million/.

[26] Dissent, *supra* note 24.

Money Message further threatened to publish the stolen data in batches if they were not paid a ransom, claiming that they would publish information from 400 databases every 48 hours.[27]

51. On April 9, 2023, when the ransom demand timer ran out, Money Message published the stolen data on their leak site, where the files are still available for download.[28] The leaked information includes patient PII and PHI.[29] Since the release of the stolen information from PharMerica, a threat actor has already posted the leaked information on "a clearnet hacking forum, breaking the file into 13 parts for easier downloading."[30]

52. Despite Money Message claiming to have stolen patient PII and PHI in March 2023, PharMerica did not begin notifying individuals impacted by the Data Breach until May 12, 2023, approximately two months after the Data Breach.

53. According to PharMerica, it discovered the Data Breach after noticing suspicious activity on its computer network on or around March 14, 2023.[31] Upon discovering the suspicious activity, PharMerica began an internal investigation and engaged cybersecurity experts.[32]

54. The investigation into the Data Breach determined that an unknown third-party gained access to Defendant's computer systems from March 12-13, 2023, and may have obtained certain personal information pertaining to Defendant's patients.[33]

---

[27] *Id.*
[28] Bill Toulas, *Ransomware gang steals data of 5.8 million PharMerica patients*, BleepingComputer (May 15, 2023), https://www.bleepingcomputer.com/news/security/ransomware-gang-steals-data-of-58-million-pharmerica-patients/.
[29] Dissent, *supra* note 24.
[30] Toulas, *supra* note 28.
[31] Notice of Data Breach, *supra* note 4.
[32] *Id.*
[33] *Id.*

55. On March 21, 2023, PharMerica identified the information compromised in the Data Breach, determining that the names, dates of birth, Social Security numbers, medication lists, and health insurance information of its patients were disclosed during the Data Breach.[34]

56. On or around May 12, 2023, PharMerica notified the U.S. Department of Health and Human Services, Office for Civil Rights of the Data Breach, indicating that the Data Breach impacted approximately 5.8 million individuals.[35]

57. On or around the same time, Plaintiff received a Data Breach notification from Defendant informing her that her PII and PHI had been compromised during the Data Breach.

58. Upon information and belief, Class Members received similar Data Breach notifications from Defendant informing them that their PII and PHI and been compromised during the Data Breach.

59. The Data Breach is the direct and proximate result of Defendant's failure to implement reasonable data security measures.

D. PharMerica Is Obligated Under HIPAA to Safeguard Patient PHI.

60. PharMerica is required by the Health Insurance Portability and Accountability Act, 42 U.S.C. § 1302d, *et seq*. ("HIPAA") to safeguard patient PHI.

61. PharMerica is an entity covered by HIPAA, which sets minimum federal standards for privacy and security of PHI.

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

---

[34] *Id.*

[35] *Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information*, U.S. Department of Health & Human Services Office for Civil Rights, https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (last visited June 6, 2023).

63. Under 45 C.F.R. §160.103, HIPAA defines "protected health information" or PHI as "individually identifiable health information" that is "transmitted by electronic media"; "[m]aintained in electronic media"; or "[t]ransmitted or maintained in any other form or medium."

64. Under 45 C.F.R. §160.103, HIPAA defines "individually identifiable health information" as "a subset of health information, including demographic information collected from an individual" that is (1) "created or received by a health care provider;" (2)"[r]elates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual;" and (3) either (a) "identifies the individual"; or (b) "[w]ith respect to which there is a reasonable basis to believe the information can be used to identify the individual."

65. HIPAA requires PharMerica to: (a) ensure the confidentiality, integrity, and availability of all electronic PHI it creates, receives, maintains, or transmits; (b) identify and protect against reasonably anticipated threats to the security or integrity of the electronic PHI; (c) protect against reasonably anticipated, impermissible uses, or disclosures of the PHI; and (d) ensure compliance by its workforce to satisfy HIPAA's security requirements. 45 C.F.R. § 164.102, *et seq*.

66. While HIPAA permits healthcare providers to disclose PHI to third parties under certain circumstances, HIPAA does not permit healthcare providers to disclose PHI to cybercriminals nor did Plaintiff or the Class Members consent to the disclosure of their PHI to cybercriminals.

67. As such, PharMerica is required under HIPAA to maintain the strictest confidentiality of Plaintiff's and Class Members' PHI that it requires, receives, and collects, and

Defendant is further required to maintain sufficient safeguards to protect that information from being accessed by unauthorized third parties.

68. Given the application of HIPAA to PharMerica, and that Plaintiff and Class Members entrusted their PHI to Defendant in order to receive medical treatment, Plaintiff and Class Members reasonably expected that Defendant would safeguard their highly sensitive information and keep their PHI confidential.

E. FTC Guidelines Prohibit PharMerica From Engaging in Unfair or Deceptive Acts or Practices.

69. PharMerica is prohibited by the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45 from engaging in "unfair or deceptive acts or practices in or affecting commerce." The Federal Trade Commission ("FTC") has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of the FTC Act.

70. The FTC has promulgated numerous guides for businesses that highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[36]

71. The FTC provided cybersecurity guidelines for businesses, advising that businesses should protect personal customer information, properly dispose of personal information that is no longer needed, encrypt information stored on networks, understand their network's vulnerabilities, and implement policies to correct any security problems.[37]

---

[36] *Start with Security – A Guide for Business*, U.S. FED. TRADE COMM'N (June 2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last visited on June 6, 2023).

[37] *Protecting Personal Information: A Guide for Business*, U.S. FED. TRADE COMM'N (Oct. 2016), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited on June 6, 2023).

72. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to private data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.[38]

73. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the FTC Act. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

74. PharMerica failed to properly implement basic data security practices. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to patient PII and PHI constitutes an unfair act of practice prohibited by Section 5 of the FTC Act.

75. PharMerica was at all times fully aware of its obligations to protect the PII and PHI of patients because of its position as a healthcare provider, which gave it direct access to reams of patient PII and PHI. Defendant was also aware of the significant repercussions that would result from its failure to do so.

F. Plaintiff and Class Members Suffered Damages.

76. For the reasons mentioned above, Defendant's conduct, which allowed the Data Breach to occur, caused Plaintiff, and members of the Class, significant injuries and harm in several ways. Plaintiff and members of the Class must immediately devote time, energy, and money to: 1) closely monitor their medical statements, bills, records, and credit and financial accounts; 2)

[38] *Id.*

change login and password information on any sensitive account even more frequently than they already do; 3) more carefully screen and scrutinize phone calls, emails, and other communications to ensure that they are not being targeted in a social engineering or spear phishing attack; and 4) search for suitable identity theft protection and credit monitoring services, and pay to procure them.

77. Once PII and PHI is exposed, there is virtually no way to ensure that the exposed information has been fully recovered or obtained against future misuse. For this reason, Plaintiff and Class Members will need to maintain these heightened measures for years, and possibly their entire lives as a result of Defendant's conduct. Further, the value of Plaintiff and Class Members' PII and PHI has been diminished by its exposure in the Data Breach.

78. As a result of Defendant's failures, Plaintiff and Class Members are at substantial increased risk of suffering identity theft and fraud or misuse of their PHI.

79. From a recent study, 28% of consumers affected by a data breach become victims of identity fraud – this is a significant increase from a 2012 study that found only 9.5% of those affected by a breach would be subject to identity fraud. Without a data breach, the likelihood of identify fraud is only about 3%.[39]

80. With respect to health care breaches, another study found "the majority [70%] of data impacted by healthcare breaches could be leveraged by hackers to commit fraud or identity theft."[40]

[39] Stu Sjouwerman, *28 Percent of Data Breaches Lead to Fraud*, KNOWBE4 (Mar. 7, 2023), https://blog.knowbe4.com/bid/252486/28-percent-of-data-breaches-lead-to-fraud.
[40] Jessica David, *70% of Data Involved in Healthcare Breaches Increases Risk of Fraud*, HEALTH IT SEC. (Sept. 25, 2019), https://healthitsecurity.com/news/70-of-data-involved-in-healthcare-breaches-increases-risk-of-fraud.

81. "Actors buying and selling PII and PHI from healthcare institutions and providers in underground marketplaces is very common and will almost certainly remain so due to this data's utility in a wide variety of malicious activity ranging from identity theft and financial fraud to crafting of bespoke phishing lures."[41]

82. The reality is that cybercriminals seek nefarious outcomes from a data breach and "stolen health data can be used to carry out a variety of crimes."[42]

83. Health information in particular is likely to be used in detrimental ways – by leveraging sensitive personal health details and diagnoses to extort or coerce someone, and serious and long-term identity theft.[43]

84. "Medical identity theft is a great concern not only because of its rapid growth rate, but because it is the most expensive and time consuming to resolve of all types of identity theft. Additionally, medical identity theft is very difficult to detect which makes this form of fraud extremely dangerous."[44]

85. Plaintiff and Class Members are also at a continued risk because their information remains in Defendant's systems, which have already been shown to be susceptible to compromise and attack and is subject to further attack so long as Defendant fails to undertake the necessary and appropriate security and training measures to protect its patients' PII and PHI.

---

[41] *Id*.
[42] Andrew Steger, *What Happens to Stolen Healthcare Data?*, HEALTHTECH (Oct. 30, 2019), https://healthtechmagazine.net/article/2019/10/what-happens-stolen-healthcare-data-perfcon.
[43] *Id*.
[44] *The Potential Damages and Consequences of Medical Identity theft and Healthcare Data Breaches*, EXPERIAN (Apr. 2010), https://www.experian.com/assets/data-breach/white-papers/consequences-medical-id-theft-healthcare.pdf (last visited June 6, 2023).

86. Plaintiff and Class Members have suffered emotional distress as a result of the Data Breach, the increased risk of identity theft and financial fraud, and the unauthorized exposure of their private medical information to strangers.

CLASS ALLEGATIONS

87. Plaintiff brings this class action on behalf of herself, and all other individuals who are similarly situated, pursuant to Rule 23 of the Federal Rules of Civil Procedure.

88. Plaintiff seeks to represent a class of persons to be defined as follows:

> All individuals in the United States and its territories whose PII and/or PHI was compromised in the PharMerica Data Breach which was announced on or about May 12, 2023 (the "Class").

89. Excluded from the Class are Defendant, its subsidiaries and affiliates, officers and directors, any entity in which Defendant has a controlling interest, the legal representative, heirs, successors, or assigns of any such excluded party, the judicial officer(s) to whom this action is assigned, and the members of their immediate families.

90. This proposed class definition is based on the information available to Plaintiff at this time. Plaintiff may modify the class definition in an amended pleading or when she moves for class certification, as necessary to account for any newly learned or changed facts as the situation develops and discovery gets underway.

91. **Numerosity:** Plaintiff is informed and believes, and thereon alleges, that there are at minimum, millions of members of the Class described above. The exact size of the Class and the identities of the individual members are identifiable through Defendant's records, including but not limited to the files implicated in the Data Breach, but based on public information, the Class includes approximately 5.8 million individuals.

92. **Commonality:** This action involved questions of law and fact common to the Class. Such common questions include but are not limited to:

a. Whether Defendant had a duty to protect the PII and PHI of Plaintiff and Class Members;

b. Whether Defendant was negligent in collecting and storing Plaintiff's and Class Members' PII and PHI, and breached its duties thereby;

c. Whether Plaintiff and Class Members are entitled to damages as a result of Defendant's wrongful conduct; and

d. Whether Plaintiff and Class Members are entitled to restitution as a result of Defendant's wrongful conduct.

93. **Typicality:** Plaintiff's claims are typical of the claims of the members of the Class. The claims of the Plaintiff and members of the Class are based on the same legal theories and arise from the same unlawful and willful conduct. Plaintiff and members of the Class were all patients of Defendant, each having their PII and PHI exposed and/or accessed by an unauthorized third party.

94. **Adequacy of Representation:** Plaintiff is an adequate representative of the Class because her interests do not conflict with the interests of the members of the Class. Plaintiff will fairly, adequately, and vigorously represent and protect the interests of the members of the Class and has no interests antagonistic to the members of the Class. In addition, Plaintiff has retained counsel who are competent and experienced in the prosecution of class action litigation. The claims of Plaintiff and the Class Members are substantially identical as explained above.

95. **Superiority:** This class action is appropriate for certification because class proceedings are superior to other available methods for the fair and efficient adjudication of this controversy and joinder of all members of the Class is impracticable. This proposed class action presents fewer management difficulties than individual litigation, and provides the benefits of

single adjudication, economies of scale, and comprehensive supervision by a single court. Class treatment will create economies of time, effort, expense, and promote uniform decision-making.

96. **Predominance:** Common questions of law and fact predominate over any questions affecting only individual Class Members. Similar or identical violations, business practices, and injuries are involved. Individual questions, if any, pale by comparison, in both quality and quantity, to the numerous common questions that dominate this action. For example, Defendant's liability and the fact of damages is common to Plaintiff and each member of the Class. If Defendant breached its duty to Plaintiff and Class Members, then Plaintiff and each Class member suffered damages by that conduct.

97. **Injunctive Relief:** Defendant has acted and/or refused to act on grounds that apply generally to the Class, making injunctive and/or declaratory relief appropriate with respect to the Class under Fed. Civ. P. 23(b)(2).

98. **Ascertainability:** Members of the Class are ascertainable. Class membership is defined using objective criteria and Class Members may be readily identified through Defendant's books and records.

FIRST CAUSE OF ACTION
NEGLIGENCE
(Plaintiff on Behalf of the Class)

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

100. Defendant owed a duty under common law to Plaintiff and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting their PII and PHI in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons.

101. PharMerica's duty to use reasonable care arose from several sources, including but not limited to those described below.

102. PharMerica has a common law duty to prevent foreseeable harm to others. This duty existed because Plaintiff and Class Members were the foreseeable and probable victims of any inadequate security practices on the part of Defendant. By receiving, maintaining, and handling PII and PHI that is routinely targeted by criminals for unauthorized access, PharMerica was obligated to act with reasonable care to protect against these foreseeable threats.

103. PharMerica's duty also arose from Defendant's position as a healthcare provider. PharMerica holds itself out as a trusted provider of medication services, thereby assuming a duty to reasonably protect the information it obtains from its patients. Indeed, Defendant, who receives, maintains, collects, and handles PII and PHI from its patients, was in a unique and superior position to protect against the harm suffered by Plaintiff and Class Members as a result of the Data Breach.

104. PharMerica breached the duties owed to Plaintiff and Class Members and was thus negligent. Although the exact methodologies employed by the unauthorized third parties are unknown to Plaintiff at this time, on information and belief, Defendant breached its duties through some combination of the following errors and omissions that allowed the data compromise to occur: (a) mismanaging its system and failing to identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that resulted in the unauthorized access and compromise of PII and PHI; (b) mishandling its data security by failing to assess the sufficiency of its safeguards in place to control these risks; (c) failing to design and implement information safeguards to control these risks; (d) failing to adequately test and monitor the effectiveness of the safeguards' key controls, systems, and procedures; (e) failing to evaluate and adjust its information security program in light of the circumstances alleged herein;

(f) failing to detect the breach at the time it began or within a reasonable time thereafter; (g) failing to follow its own privacy policies and practices published to its patients; and (h) failing to adequately train and supervise employees and third party vendors with access or credentials to systems and databases containing sensitive PII or PHI.

105. But for Defendant's wrongful and negligent breach of its duties owed to Plaintiff and Class Members, their PII and PHI would not have been compromised.

106. As a direct and proximate result of Defendant's negligence, Plaintiff and Class Members have suffered injuries, including:

a. Theft of their PII and/or PHI;

b. Costs associated with the detection and prevention of identity theft and unauthorized use of the financial accounts;

c. Costs associated with purchasing credit monitoring and identity theft protection services;

d. Lowered credit scores resulting from credit inquiries following fraudulent activities;

e. Costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Data Breach – including finding fraudulent charges, cancelling and reissuing cards, enrolling in credit monitoring and identity theft protection services, freezing and unfreezing accounts, and imposing withdrawal and purchase limits on compromised accounts;

f. The imminent and certainly impending injury flowing from the increased risk of potential fraud and identity theft posed by their PII and/or PHI being placed in the hands of criminals;

g. Damages to and diminution in value of their PII and PHI entrusted, directly or indirectly, to Defendant with the mutual understanding that Defendant would safeguard Plaintiff's and Class Members' data against theft and not allow access and misuse of their data by others;

h. Continued risk of exposure to hackers and thieves of their PII and/or PHI, which remains in Defendant's possession and is subject to further breaches so long as Defendant fail to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' data; and

i. Emotional distress from the unauthorized disclosure of PII and PHI to strangers who likely have nefarious intentions and now have prime opportunities to commit identity theft, fraud, and other types of attacks on Plaintiff and Class members.

107. As a direct and proximate result of Defendant's negligence, Plaintiff and Class Members are entitled to damages, including compensatory, punitive, and/or nominal damages, in an amount to be proven at trial.

SECOND CAUSE OF ACTION
NEGLIGENCE PER SE
(Plaintiff on Behalf of the Class)

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

109. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce" including, as interpreted and enforced by the FTC, the unfair act or practice by entities such as

Defendant for failing to use reasonable measures to protect PII and PHI. Various FTC publications and orders also form the basis of PharMerica's duty.

110. PharMerica violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and PHI and not complying with the industry standards. Defendant's conduct was particularly unreasonable given the nature and amount of PII and PHI it obtained and stored and the foreseeable consequences of a data breach involving the PII and PHI it entrusted from its patients.

111. Plaintiff and members of the Class are consumers within the class of persons Section 5 of the FTC Act was intended to protect.

112. Defendant's violation of Section 5 of the FTC Act constitutes negligence *per se*.

113. PharMerica is an entity covered under the HIPAA, which sets minimum federal standards for privacy and security of PHI.

114. Pursuant to HIPAA, 42 U.S.C. § 1302d, *e. seq.*, and its implementing regulations, Defendant had a duty to implement and maintain reasonable and appropriate administrative, technical, and physical safeguards to protect Plaintiff's and the Class members' electronic PHI.

115. Specifically, HIPAA required Defendant to: (a) ensure the confidentiality, integrity, and availability of all electronic PHI it creates, receives, maintains, or transmits; (b) identify and protect against reasonably anticipated threats to the security or integrity of the electronic PHI; (c) protect against reasonably anticipated, impermissible uses, or disclosures of the PHI; and (d) ensure compliance by its workforce to satisfy HIPAA's security requirements. 45 CFR § 164.102, *et seq*.

116. Defendant violated HIPAA by actively disclosing Plaintiff's and the Class Members' electronic PHI; by failing to provide fair, reasonable, or adequate computer systems and

data security practices to safeguard Plaintiff's and Class Members' PHI; and by failing to timely notify Plaintiff and Class Members of a breach of their PHI.

117. Plaintiff and the Class Members are patients within the class of persons HIPAA was intended to protect, as they are patients of PharMerica.

118. Defendant's violation of HIPAA constitutes negligence *per se*.

119. The harm that has occurred as a result of Defendant's conduct is the type of harm that the FTC Act and HIPAA were intended to guard against.

120. As a direct and proximate result of Defendant's negligence, Plaintiff and Class Members have suffered injuries, including:

a. Theft of their PII and/or PHI;

b. Costs associated with the detection and prevention of identity theft and unauthorized use of the financial accounts;

c. Costs associated with purchasing credit monitoring and identity theft protection services;

d. Lowered credit scores resulting from credit inquiries following fraudulent activities;

e. Costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Data Breach – including finding fraudulent charges, cancelling and reissuing cards, enrolling in credit monitoring and identity theft protection services, freezing and unfreezing accounts, and imposing withdrawal and purchase limits on compromised accounts;

f. The imminent and certainly impending injury flowing from the increased risk of potential fraud and identity theft posed by their PII and/or PHI being placed in the hands of criminals;

g. Damages to and diminution in value of their PII and PHI entrusted, directly or indirectly, to Defendant with the mutual understanding that Defendant would safeguard Plaintiff's and Class Members' data against theft and not allow access and misuse of their data by others;

h. Continued risk of exposure to hackers and thieves of their PII and/or PHI, which remains in Defendant's possession and is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' data; and

i. Emotional distress from the unauthorized disclosure of PII and PHI to strangers who likely have nefarious intentions and now have prime opportunities to commit identity theft, fraud, and other types of attacks on Plaintiff and Class members.

121. As a direct and proximate result of Defendant's negligence, Plaintiff and Class Members have been injured as described herein, and are entitled to damages, including compensatory, punitive, and nominal damages, in an amount to be proven at trial.

THIRD CAUSE OF ACTION
BREACH OF IMPLIED CONTRACT
(Plaintiff on Behalf of the Class)

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

123. Plaintiff brings this claim individually and on behalf of the Class.

124. When Plaintiff and members of the Class provided their PII and PHI to PharMerica in exchange for medication services, they entered into implied contracts with Defendant, under which PharMerica agreed to take reasonable steps to protect Plaintiff's and Class Members' PII and PHI, comply with it statutory and common law duties to protect Plaintiff's and Class Members' PII and PHI, and to timely notify them in the event of a data breach.

125. PharMerica solicited and invited Plaintiff and Class Members to provide their PII and PHI as part of Defendant's provision of medication services. Plaintiff and Class Members accepted Defendant's offers when they made and paid for purchases of Defendant's services and products and provided their PII and PHI to Defendant.

126. When entering into implied contracts, Plaintiff and Class Members reasonably believed and expected that Defendant's data security practices complied with its statutory and common law duties to adequately protect Plaintiff's and Class Members' PII and PHI and to timely notify them in the event of a data breach.

127. PharMerica's implied promise to safeguard patient PII and PHI is evidenced by, *e.g.*, the representations in Defendant's Notice of Privacy Practices set forth above.

128. Plaintiff and Class Members paid money to PharMerica to receive healthcare services. Plaintiff and Class Members reasonably believed and expected that Defendant would use part of those funds to obtain adequate data security. PharMerica failed to do so.

129. Plaintiff and Class Members would not have provided their PII and PHI to PharMerica had they known that Defendant would not safeguard their PII and PHI, as promised, or provide timely notice of a data breach.

130. Plaintiff and Class Members fully performed their obligations under their implied contracts with PharMerica.

131. PharMerica breached its implied contracts with Plaintiff and Class Members by failing to safeguard Plaintiff's and Class Members' PII and PHI.

132. The losses and damages Plaintiff and Class Members sustained, include, but are not limited to:

a. Theft of their PII and/or PHI;

b. Costs associated with purchasing credit monitoring and identity theft protection services;

c. Costs associated with the detection and prevention of identity theft and unauthorized use of their PII and PHI;

d. Lowered credit scores resulting from credit inquiries following fraudulent activities;

e. Costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Data Breach – including finding fraudulent charges, cancelling and reissuing cards, enrolling in credit monitoring and identity theft protection services, freezing and unfreezing accounts, and imposing withdrawal and purchase limits on compromised accounts;

f. The imminent and certainly impending injury flowing from the increased risk of potential fraud and identity theft posed by their PII and/or PHI being placed in the hands of criminals;

g. Damages to and diminution in value of their PII and PHI entrusted, directly or indirectly, to Defendant with the mutual understanding that Defendant

would safeguard Plaintiff's and Class Members' data against theft and not allow access and misuse of their data by others;

h. Continued risk of exposure to hackers and thieves of their PII and/or PHI, which remains in Defendant's possession and is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' data; and

i. Emotional distress from the unauthorized disclosure of PII and PHI to strangers who likely have nefarious intentions and now have prime opportunities to commit identity theft, fraud, and other types of attacks on Plaintiff and Class Members.

133. As a direct and proximate result of Defendant's breach of contract, Plaintiff and Class Members are entitled to damages, including compensatory, punitive, and/or nominal damages, in an amount to be proven at trial.

FOURTH CAUSE OF ACTION
UNJUST ENRICHMENT
(Plaintiff on Behalf of the Class)

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

135. Plaintiff brings this claim individually and on behalf of the Class in the alternative to Plaintiff's Breach of Implied Contract claim.

136. Upon information and belief, Defendant funds its data security measures entirely from its general revenue, including payments made by or on behalf of Plaintiff and the Class Members.

137. As such, a portion of the payments made by or on behalf of Plaintiff and the Class Members is to be used to provide a reasonable level of data security, and the amount of the portion of each payment made that is allocated to data security is known to Defendant.

138. Plaintiff and Class Members conferred a monetary benefit on Defendant. Specifically, they purchased healthcare services from Defendant and/or its agents and in so doing provided Defendant with their PII and PHI. In exchange, Plaintiff and Class Members should have received from Defendant the goods and services that were the subject of the transaction and have their PII and PHI protected with adequate data security.

139. Defendant knew that Plaintiff and Class Members conferred a benefit which Defendant accepted. Defendant profited from these transactions and used the PII and PHI of Plaintiff and Class Members for business purposes.

140. In particular, Defendant enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiff's and Class Members' PII and PHI. Instead of providing a reasonable level of security that would have prevented the Data Breach, Defendant instead calculated to increase its own profits at the expense of Plaintiff and Class Members by utilizing cheaper, ineffective security measures. Plaintiff and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's decision to prioritize its own profits over the requisite security.

141. Under the principles of equity and good conscience, Defendant should not be permitted to retain the money belonging to Plaintiff and Class Members, because Defendant failed to implement appropriate data management and security measures that are mandated by its common law and statutory duties.

142. Defendant failed to secure Plaintiff and Class Members' PII and PHI and, therefore, did not provide full compensation for the benefit Plaintiff and Class Members provided.

143. Defendant acquired the PII and PHI through inequitable means in that it failed to disclose the inadequate security practices previously alleged.

144. If Plaintiff and Class Members knew that Defendant had not reasonably secured their PII and PHI, they would not have agreed to provide their PII and PHI to Defendant.

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

146. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have sustained injuries, including, but not limited to:

a. Theft of their PII and/or PHI;

b. Costs associated with purchasing credit monitoring and identity theft protection services;

c. Costs associated with the detection and prevention of identity theft and unauthorized use of their PII and PHI;

d. Lowered credit scores resulting from credit inquiries following fraudulent activities;

e. Costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Data Breach – including finding fraudulent charges, cancelling and reissuing cards, enrolling in credit monitoring and identity theft protection services, freezing and unfreezing accounts, and imposing withdrawal and purchase limits on compromised accounts;

f. The imminent and certainly impending injury flowing from the increased risk of potential fraud and identity theft posed by their PII and/or PHI being placed in the hands of criminals;

g. Damages to and diminution in value of their PII and PHI entrusted, directly or indirectly, to Defendant with the mutual understanding that Defendant would safeguard Plaintiff's and Class Members' data against theft and not allow access and misuse of their data by others;

h. Continued risk of exposure to hackers and thieves of their PII and/or PHI, which remains in Defendant's possession and is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' data; and

i. Emotional distress from the unauthorized disclosure of PII and PHI to strangers who likely have nefarious intentions and now have prime opportunities to commit identity theft, fraud, and other types of attacks on Plaintiff and Class Members.

147. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered damages and will continue to suffer other forms of injury and/or harm.

148. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and Class Members, proceeds that they unjustly received from them. In the alternative, Defendant should be compelled to refund the amounts that Plaintiff and Class Members overpaid for Defendant's services.

FIFTH CAUSE OF ACTION
DECLARATORY JUDGMENT
(Plaintiff on Behalf of the Class)

149. Plaintiff restates and realleges all preceding allegations above as if fully set forth herein.

150. 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 federal and state statutes described in this Complaint.

151. An actual controversy has arisen in the wake of the Data Breach regarding Plaintiff's and Class Members' PII and PHI, which remains in Defendant's possession, and whether Defendant is currently maintaining data security measures adequate to protect Plaintiff and Class Members from further data breaches that compromise their PII and PHI. Plaintiff alleges that PharMerica's data security measures remain inadequate. Furthermore, Plaintiff continues to suffer injury as a result of the compromise of her PII and PHI and remains at imminent risk that further compromises of her PII and/or PHI will occur in the future.

152. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. Defendant owed a legal duty to secure patients' PII and PHI under the common law, Section 5 of the FTC Act, and HIPAA; and

b. Defendant breached and continues to breach this legal duty by failing to employ reasonable measures to secure consumers' PII and PHI.

153. This Court also should issue corresponding prospective injunctive relief requiring Defendant to employ adequate security protocols consistent with law and industry standards to protect patients' PII and PHI.

154. If an injunction is not issued, Plaintiff and Class Members will suffer irreparable injury, and lack an adequate legal remedy, in the event of another data breach at PharMerica. The risk of another such breach is real, immediate, and substantial. If another breach at PharMerica occurs, Plaintiff will not have an adequate remedy at law because many of the resulting injuries are not readily quantified, and she will be forced to bring multiple lawsuits to rectify the same conduct.

155. The hardship to Plaintiff and Class Members if an injunction is not issued exceeds the hardship to Defendant if an injunction is issued. Plaintiff will likely be subjected to substantial identity theft and other damage. On the other hand, the cost to Defendant 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.

156. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach at PharMerica, thus eliminating the additional injuries that would result to Plaintiff, Class Members, and patients whose confidential information would be further compromised.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of herself and all other similarly situated, prays for relief as follows:

A. For an order certifying the Class under Rule 23 of the Federal Rules of Civil Procedure and naming Plaintiff as representative of the Class and Plaintiff's attorneys as Class Counsel to represent the Class;

B. For an order finding in favor of Plaintiff and the Class on all counts asserted herein;

C. For damages in an amount to be determined by the trier of fact;

D. For an order of restitution and all other forms of equitable monetary relief;

E. Declaratory and injunctive relief as described herein;

F. Awarding Plaintiff's reasonable attorneys' fees, costs, and expenses;

G. Awarding pre- and post-judgment interest on any amounts awarded; and

H. Awarding such other and further relief as may be just and proper.

JURY TRIAL DEMANDED

A jury trial is demanded on all claims so triable.

Dated: June 8, 2023

Respectfully submitted,

/s/ Joseph M. Lyon
Joseph M. Lyon
THE LYON FIRM
2754 Erie Ave.
Cincinnati, OH 45208
Phone: (513) 381-2333
Fax: (513) 766-9011
Email: *jlyon@thelyonfirm.com*

Gary F. Lynch*
Jamisen A. Etzel*
Nicholas A. Colella
LYNCH CARPENTER LLP
1133 Penn Avenue, 5th Floor
Pittsburgh, PA 15222
Telephone: (412) 322-9243
Facsimile: (412) 231-0246
gary@lcllp.com
jamisen@lcllp.com
nickc@lcllp.com

**pro hac vice forthcoming*

Attorneys for Plaintiff

JS 44 (Rev. 10/20)

CIVIL COVER SHEET

3:23CV-297-RGJ

The JS 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 by the Judicial Conference of the United States in September 1974, is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. *(SEE INSTRUCTIONS ON NEXT PAGE OF THIS FORM.)*

I. (a) PLAINTIFFS

Jaketrius Lurry

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

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

See attachment

DEFENDANTS

Pharmerica Corporation

County of Residence of First Listed Defendant Jefferson
(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)*

Click here for: Nature of Suit Code Descriptions.

CONTRACT
- 110 Insurance
- 120 Marine
- 130 Miller Act
- 140 Negotiable Instrument
- 150 Recovery of Overpayment & Enforcement of Judgment
- 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 and Corrupt Organizations
- 480 Consumer Credit (15 USC 1681 or 1692)
- 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)***:
28 U.S.C. § 1332(d)(2)(A); 28 U.S.C. §§2201

Brief description of cause:
Data breach class action

VII. REQUESTED IN COMPLAINT:

■ CHECK IF THIS IS A **CLASS ACTION** UNDER RULE 23, F.R.Cv.P.

DEMAND $ > $5,000,000

CHECK YES only if demanded in complaint:

JURY DEMAND: ■ Yes ☐ No

VIII. RELATED CASE(S) IF ANY

(See instructions): JUDGE _____ DOCKET NUMBER _____

DATE
June 8, 2023

SIGNATURE OF ATTORNEY OF RECORD
/s/ Joseph M. Lyon

FOR OFFICE USE ONLY

RECEIPT # _____ AMOUNT _____ APPLYING IFP _____ JUDGE _____ MAG. JUDGE _____

INSTRUCTIONS FOR ATTORNEYS COMPLETING CIVIL COVER SHEET FORM JS 44

Authority For Civil Cover Sheet

The JS 44 civil cover sheet and the information contained herein neither replaces nor supplements the filings and service of pleading or other papers as required by law, except as provided by local rules of court. This form, approved by the Judicial Conference of the United States in September 1974, is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. Consequently, a civil cover sheet is submitted to the Clerk of Court for each civil complaint filed. The attorney filing a case should complete the form as follows:

I.(a) Plaintiffs-Defendants. Enter names (last, first, middle initial) of plaintiff and defendant. If the plaintiff or defendant is a government agency, use only the full name or standard abbreviations. If the plaintiff or defendant is an official within a government agency, identify first the agency and then the official, giving both name and title.

(b) County of Residence. For each civil case filed, except U.S. plaintiff cases, enter the name of the county where the first listed plaintiff resides at the time of filing. In U.S. plaintiff cases, enter the name of the county in which the first listed defendant resides at the time of filing. (NOTE: In land condemnation cases, the county of residence of the "defendant" is the location of the tract of land involved.)

(c) Attorneys. Enter the firm name, address, telephone number, and attorney of record. If there are several attorneys, list them on an attachment, noting in this section "(see attachment)".

II. Jurisdiction. The basis of jurisdiction is set forth under Rule 8(a), F.R.Cv.P., which requires that jurisdictions be shown in pleadings. Place an "X" in one of the boxes. If there is more than one basis of jurisdiction, precedence is given in the order shown below.
United States plaintiff. (1) Jurisdiction based on 28 U.S.C. 1345 and 1348. Suits by agencies and officers of the United States are included here.
United States defendant. (2) When the plaintiff is suing the United States, its officers or agencies, place an "X" in this box.
Federal question. (3) This refers to suits under 28 U.S.C. 1331, where jurisdiction arises under the Constitution of the United States, an amendment to the Constitution, an act of Congress or a treaty of the United States. In cases where the U.S. is a party, the U.S. plaintiff or defendant code takes precedence, and box 1 or 2 should be marked.
Diversity of citizenship. (4) This refers to suits under 28 U.S.C. 1332, where parties are citizens of different states. When Box 4 is checked, the citizenship of the different parties must be checked. (See Section III below**; NOTE: federal question actions take precedence over diversity cases.**)

III. Residence (citizenship) of Principal Parties. This section of the JS 44 is to be completed if diversity of citizenship was indicated above. Mark this section for each principal party.

IV. Nature of Suit. Place an "X" in the appropriate box. If there are multiple nature of suit codes associated with the case, pick the nature of suit code that is most applicable. Click here for: Nature of Suit Code Descriptions.

V. Origin. Place an "X" in one of the seven boxes.
Original Proceedings. (1) Cases which originate in the United States district courts.
Removed from State Court. (2) Proceedings initiated in state courts may be removed to the district courts under Title 28 U.S.C., Section 1441.
Remanded from Appellate Court. (3) Check this box for cases remanded to the district court for further action. Use the date of remand as the filing date.
Reinstated or Reopened. (4) Check this box for cases reinstated or reopened in the district court. Use the reopening date as the filing date.
Transferred from Another District. (5) For cases transferred under Title 28 U.S.C. Section 1404(a). Do not use this for within district transfers or multidistrict litigation transfers.
Multidistrict Litigation – Transfer. (6) Check this box when a multidistrict case is transferred into the district under authority of Title 28 U.S.C. Section 1407.
Multidistrict Litigation – Direct File. (8) Check this box when a multidistrict case is filed in the same district as the Master MDL docket.
PLEASE NOTE THAT THERE IS NOT AN ORIGIN CODE 7. Origin Code 7 was used for historical records and is no longer relevant due to changes in statue.

VI. Cause of Action. Report the civil statute directly related to the cause of action and give a brief description of the cause. **Do not cite jurisdictional statutes unless diversity.** Example: U.S. Civil Statute: 47 USC 553 Brief Description: Unauthorized reception of cable service.

VII. Requested in Complaint. Class Action. Place an "X" in this box if you are filing a class action under Rule 23, F.R.Cv.P.
Demand. In this space enter the actual dollar amount being demanded or indicate other demand, such as a preliminary injunction.
Jury Demand. Check the appropriate box to indicate whether or not a jury is being demanded.

VIII. Related Cases. This section of the JS 44 is used to reference related pending cases, if any. If there are related pending cases, insert the docket numbers and the corresponding judge names for such cases.

Date and Attorney Signature. Date and sign the civil cover sheet.

Joseph M. Lyon
THE LYON FIRM
2754 Erie Ave.
Cincinnati, OH 45208
Phone: (513) 381-2333
Fax: (513) 766-9011
Email: jlyon@thelyonfirm.com

Gary F. Lynch*
Jamisen A. Etzel*
Nicholas A. Colella
LYNCH CARPENTER LLP
1133 Penn Avenue, 5th Floor
Pittsburgh, PA 15222
Telephone: (412) 322-9243
Facsimile: (412) 231-0246
gary@lcllp.com
jamisen@lcllp.com
nickc@lcllp.com

*pro hac vice forthcoming

Attorneys for Plaintiff

AO 440 (Rev. 06/12) Summons in a Civil Action

UNITED STATES DISTRICT COURT

for the

Western District of Kentucky

JAKETRIUS LURRY, on behalf of herself and all others similarly situated,

Plaintiff(s)

v.

PHARMERICA CORPORATION

Defendant(s)

Civil Action No. 3:23CV-297-RGJ

SUMMONS IN A CIVIL ACTION

To: *(Defendant's name and address)* Pharmerica Corporation
805 N. Whittington Parkway,
Louisville, Kentucky 40222

ALSO SERVE:
Corporation Service Company
421 WEST MAIN STREET
FRANKFORT, KY 40601

A lawsuit has been filed against you.

Within 21 days after service of this summons on you (not counting the day you received it) — or 60 days if you are the United States or a United States agency, or an officer or employee of the United States described in Fed. R. Civ. P. 12 (a)(2) or (3) — you must serve on the plaintiff an answer to the attached complaint or a motion under Rule 12 of the Federal Rules of Civil Procedure. The answer or motion must be served on the plaintiff or plaintiff's attorney, whose name and address are:

Joseph M. Lyon
THE LYON FIRM
2754 Erie Ave.
Cincinnati, OH 45208
Phone: (513) 381-2333
Fax: (513) 766-9011
Email: jlyon@thelyonfirm.com

If you fail to respond, judgment by default will be entered against you for the relief demanded in the complaint. You also must file your answer or motion with the court.

CLERK OF COURT

Date: _____

_____
Signature of Clerk or Deputy Clerk

Civil Action No. 3:23CV-297-RGJ

PROOF OF SERVICE

(This section should not be filed with the court unless required by Fed. R. Civ. P. 4 (l))

This summons for *(name of individual and title, if any)* _____ was received by me on *(date)* _____ .

❒ I personally served the summons on the individual at *(place)* _____ on *(date)* _____ ; or

❒ I left the summons at the individual's residence or usual place of abode with *(name)* _____ , a person of suitable age and discretion who resides there, on *(date)* _____ , and mailed a copy to the individual's last known address; or

❒ I served the summons on *(name of individual)* _____ , who is designated by law to accept service of process on behalf of *(name of organization)* _____ on *(date)* _____ ; or

❒ I returned the summons unexecuted because _____ ; or

❒ Other *(specify):*

My fees are $ _____ for travel and $ _____ for services, for a total of $ 0.00 .

I declare under penalty of perjury that this information is true.

Date: _____

_____
Server's signature

_____
Printed name and title

_____
Server's address

Additional information regarding attempted service, etc:

Print Save As... Reset