Exhibit A

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

In Re: PharMerica Data Breach Litigation This Document Relates To: **All Actions**	Master File No. 3:23-cv-00297-RGJ **FIRST AMENDED CONSOLIDATED CLASS ACTION COMPLAINT** **JURY TRIAL DEMAND**

FIRST AMENDED CONSOLIDATED CLASS ACTION COMPLAINT

Plaintiffs David Hibbard, Frank Raney, James Young, Holly Williams, Micaela Molina and Charley Luther ("Plaintiffs") bring this First Amended Consolidated Class Action Complaint ("Complaint") against PharMerica Corporation ("PharMerica" or "Defendant"), as individuals, and on behalf of all others similarly situated, and allege, upon personal knowledge as to their own actions and their counsels' investigation, and upon information and belief as to all other matters, as follows:

NATURE OF THE ACTION

1. This class action arises out of the recent cyberattack and data breach ("Data Breach") resulting from PharMerica's failure to implement reasonable and industry standard data security practices.

2. PharMerica is a nationwide provider of pharmacy services and operates 180 local and 70,000 backup pharmacies and serves healthcare partners and patients in over 3,100 long-term care, senior living, IDD/behavioral health, home infusion, specialty pharmacy, and hospital management programs.[1]

[1] https://pharmerica.com/who-we-are/

3. As part of its regular business activities PharMerica collected and maintained personal identifiable information ("PII") and protected health information ("PHI" and together with PII, "Personal Information") of Plaintiffs and the putative Class Members (defined below), who are (or were) patients and/or employees at PharMerica or entities that contracted with PharMerica.

4. Plaintiffs' and Class Members' sensitive Personal Information—which they entrusted to Defendant on the mutual understanding that Defendant would protect it against disclosure—was targeted, compromised, and unlawfully accessed by unauthorized parties due to the Data Breach.

5. In March of 2023 a cybercriminal ransomware gang known as "Money Message" targeted and breached PharMerica's computer network and exfiltrated 4.7 terabytes of information, including the sensitive personal and medical information of nearly 6 million of its own and its healthcare partners' patients. On March 28, 2023, Money Message claimed responsibility for the attack[2] and posted on the dark web a sample of the patient information they had exfiltrated from PharMerica, including "a patient-related table with name, SSN, date of birth, Medicaid number, and Medicare number, [] an Excel file with [] name, date of birth, SSN, Medicaid Number, Medicare Number, allergies, and a field with somewhat detailed diagnoses information and history."[3]

6. The data exfiltrated by Money Message during the Data Breach included at least Plaintiffs' and Class Members' full names, addresses, dates of birth, Social Security numbers, and

[2] *See* Exhibit A for the message and updates from their Dark Web posting
[3]Data Breaches.Net, *PharMerica and BrightSpring Health Services hit by Money Message (update2)*, April 8, 2023, available at https://www.databreaches.net/pharmerica-and-brightspring-health-services-hit-by-money-message/

medical and health insurance information (collectively, "Personal Information"), which is protected health information as defined by the Health Insurance Portability and Accountability Act of 1996 ("HIPAA").[4]

7. The file "granted to be top 100.xlsx" referenced in the posting from the Money Message gang, contains a spreadsheet of patient records including the following data points: ID, SSN, FirstName, MI, LastName, County, DOB, MaritalStatus, Sex, MedicaidNum, Disabled, PhysicianID, AltPhysicianID, Religion, AllergiesText, DiagnosesText.

8. The link "2nd_portion" contained in the posting from the Money Message gang contained two files, one an export from a database containing the following datapoints: id, patientid, categoryid, firstname, lastname, address1, address2, city, state, postal_code, home_phone, cell_phone, work_phone, mi, and relationship. The other file contained another export from the database containing the following datapoints: ID, SSN, PatientiCode, FirstName, MI, LastName, County, DOB, MaritalStatus, LevelOfService, Birthplace, Sex, MedicaidNum, MedicareNum, OtherInsNum, OtherInsGroupNum, Comments, Disabled, PhysicianID, AltPhysicianID, DentistID, DiagnosisID, PharmacyID, Payer, Hospital, EducationLevel, FuneralHome, RehabPotential, Diagnosis, DiagnosisText, Prognosis, Religion, AdmittedFrom, DatesOfStay1, DatesOfStay2, Nickname, Race, AmbulancePreference, PreviousOccupation, PatientAware, NameOfChurch, PharmacyMPS, PharmacyOutside, AdmissionNumber, Photo, MedicaidEffectiveDate, AllergiesText, DiagnosesText, TestPatient, Notes. These two files were labeled according to the database from which they were exported to show PharMerica the attackers had access to the entire database and give credibility to their promise to publish the entire database

[4] *See* PharMerica Notifies Individuals of Privacy Incident, available at https://pharmerica.com/data-privacy-incident/

of 4.7TB. These two files where labeled "[MethodistVillageAL].[dbo].[Address].txt" and "[MethodistVillageAL].[dbo].[Patient]."

9. The next link contained two files. "[FWDB] 500GB - Tables List.txt" is a listing of 934 tables of PharMerica's database demonstrating Money Message had access to all of the database. (*See Exhibit B - [FWDB] 500GB - Tables List*) The other file, xxxxxxxxxxxx, what an export from a query demonstrating Money Message had access to the entire dataset of 500 patients ordered by admit date containing the following datapoints: "FacID, PatID, PatLName, PatFName, MedCond, Allergy, Floor, NsID, Room, MedShtNotice, PhOrdNotice, PhNPI, PhNPI2, PatStatus, SSN, MedRecNo, BirthDate, AdmDate, Sex, NxtVisDt, NxtVisIncr, NxtVisIncrType, WeightLbs, HeightInches, Location, Religion, CareLvlCd, AllowRefills, CustomerNo, FamID, Street1, Street2, City, State, Zip Phone, InvoiceGrp, QBCustomerName, PsuedoPatient, HIPAAStmt, HIPAAStmtRecd, HIPAAStmtExpireDt, PatMI, SafetyCap, DischargeDt, Bed, UserField, DefProfileOnly, DoNotPrintMedRecs, Nickname, DeathDate, MTMFee, PreferUD, PreferNonUD, MedicareNo, DrugAllergy, OtherAllergy, DefPackType, PictureFileName, SLXPATIENTCONTACTID, UPSSvcID, UPSBillOptID, UPSPackTypeID, ExternalPatId, ReviewReqd, StatusNameCd, DeliveryRoute, DeliveryInstructions, NoCycleFill, BodySurfaceArea, GestationalAge, WeightKgs, HeightCM, PatGuid, DefDelivID, NoOTC, MaritalStatus, UsePatPackType, LICSLevel, LICSTerminationDt, LICSPlanType, DischargeReason, DefaultExempt340B, ts, StopId, ToteScanLevel, SendProofOfDelivery, DeliveryMethod, DeliveryFax, DeliveryEmail, GuardianType, GuardianFName, GuardianLName, County, Race, Ethnicity, MotherMaidenName, LanguageTranslation, LastModifiedBy.

10. As a result of the Data Breach, Plaintiff and approximately 5.8 million similarly

situated Class Members[5] suffered concrete injuries in fact including, but not limited to: (i) invasion of privacy; (ii) theft of and fraudulent use of their Personal Information; (iii) lost or diminished value of their Personal Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) experiencing an increase in spam calls, texts, and/or emails; (viii) Plaintiff Raney's Personal Information being disseminated on the dark web; (ix) statutory damages; (x) nominal damages; and (xi) the continued and certainly increased risk to their Personal Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Personal Information.

11. The Data Breach was the direct result of Defendant's failure to implement adequate and reasonable cyber-security procedures and protocols necessary to protect the Personal Information of Plaintiffs and Class Members from a foreseeable and preventable cyber-attack.

12. Defendant maintained its computer properties and the Personal Information stored thereon in a reckless manner. In particular, the Personal Information was maintained on Defendant's computer network in a condition vulnerable to cyberattacks. The threat of the cyberattack and the potential for improper disclosure of Plaintiffs' and Class Members' Personal Information was a known risk to Defendant and, thus, Defendant was on notice that failing to

[5] https://apps.web.maine.gov/online/aeviewer/ME/40/08d6080b-afcf-4d02-ba20-24f639aaca61.shtml (last accessed Jan. 8, 2024).

take steps necessary to secure the Personal Information from those risks left that Personal Information in a dangerous condition.

13. Defendant disregarded the rights of Plaintiffs and Class Members by, *inter alia*, intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure its data systems were protected against unauthorized intrusions; failing to disclose that it did not have adequately robust computer systems and security practices sufficient to safeguard Class Members' Personal Information; failing to take standard and reasonably available steps to prevent the Data Breach; and failing to provide Plaintiffs and Class Members prompt and accurate notice of the Data Breach.

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

15. Moreover, the Money Message gang has already made publicly available unencrypted and unredacted samples of the Personal Information that it exfiltrated from PharMerica's network during the Data Breach further demonstrating the present and continuing threat of identity theft faced by Plaintiffs and Class Members.

16. As a result of the Data Breach, Plaintiffs and Class Members have been exposed to a present and continuing risk of fraud and identity theft. Plaintiffs and Class Members must now and in the future closely monitor their financial accounts to guard against identity theft.

17. Plaintiffs and Class Members will also incur out of pocket costs, e.g., for purchasing credit monitoring services, credit freezes, credit reports, or other protective and mitigative measures to deter and detect identity theft.

18. Plaintiffs bring this class action lawsuit on behalf all those similarly situated to address Defendant's inadequate safeguarding of the Personal Information that it collected and maintained, and for failing to provide timely and adequate notice to Plaintiffs and other Class Members that their information had been subject to the unauthorized access by a known criminal group and precisely what specific type of information was accessed.

19. Through this Complaint, Plaintiffs seek to remedy these harms on behalf of themselves and all similarly situated individuals whose Personal Information was accessed during the Data Breach. Accordingly, Plaintiffs bring this action against Defendant seeking redress for its unlawful conduct and assert claims for: (i) negligence; (ii) negligence *per se*; (iii) breach of third-party beneficiary contract; (iv) breach of fiduciary duty; (v) unjust enrichment; (vi) violation of Kentucky's Consumer Protection Act; (vii) violation of Michigan's Data Breach Prompt Notification Law; (viii) violation of California's Unfair Competition Law; (ix) violation of the California Consumer Records Act; (x) violation of the California Consumer Privacy Act; and (xi) violation of the California Confidentiality of Medical Information Act.

PARTIES

20. Plaintiff, David Hibbard, is a resident and citizen of the Commonwealth of Kentucky.

21. Plaintiff, Frank Raney, is a resident and citizen of the State of Texas.

22. Plaintiff, James Young, is a resident and citizen of the State of Michigan.

23. Plaintiff, Holly Williams, is a resident and citizen of the State of South Carolina.

24. Plaintiff, Micaela Molina, is a resident and citizen of the State of California.

25. Plaintiff, Charley Luther, is a resident and citizen of the State of California.

26. Defendant, PharMerica, is a Delaware Corporation, with its principal place of business at 805 N. Whittington Parkway, Louisville, Kentucky 40222. Defendant is a citizen of Kentucky and Delaware. PharMerica is full-service pharmacy providing services to health care entities and individuals across the country.

JURISDICTION AND VENUE

27. This Court has subject matter jurisdiction over this action under 28 U.S.C.§ 1332(d) because this is a class action wherein the amount in controversy exceeds the sum or value of $5,000,000, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one member of the class is a citizen of a state different from Defendant.[6]

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

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

FACTUAL ALLEGATIONS

A. Defendant's Business and the Data Breach

30. PharMerica is a nationwide provider of pharmacy services and operates 180 local and 70,000 backup pharmacies and serves healthcare partners and patients in over 3,100 long-

[6] For instance, according to the report submitted to the Office of the Maine Attorney General, 40,248 Maine residents were impacted in the Data Breach. *See* https://apps.web.maine.gov/online/aeviewer/ME/40/08d6080b-afcf-4d02-ba20-24f639aaca61.shtml

term care, senior living, IDD/behavioral health, home infusion, specialty pharmacy, and hospital management programs.[7]

31. To perform its services, PharMerica requires that its employees as well as patients and those of its healthcare partners entrust it with their Personal Information, and PharMerica collects and stores that Personal Information in the regular course of its business.

32. In the course of collecting Personal Information from patients and employees, including Plaintiffs and the proposed Class Members, Defendant promised to take steps to maintain the confidentiality of that Personal Information and provide adequate security for it through its applicable privacy policy and other disclosures in compliance with industry standards, HIPAA and FTC regulations and/or guidelines, and statutory privacy requirements.

33. For instance, the Privacy Policy posted on Defendant's website promises that: "We are committed to protecting privacy of your medical information" and that it is required to provide all patients with "Notice about our legal duties and privacy practices with respect to your medical information."[8]

34. Plaintiffs and Class Members, as former and current patients of Defendant, current and former employees at Defendant, or of healthcare providers that utilize Defendant's services, relied on these and other promises and on PharMerica, a sophisticated business entity, to keep their sensitive Personal Information confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information. Patients, in general, demand security to safeguard their Personal Information, especially when PHI and other sensitive Personal Information is involved.

[7] https://pharmerica.com/who-we-are/
[8] https://pharmerica.com/privacy-policy/

35. In the course of their relationship with PharMerica, Plaintiffs and Class Members, entrusted Defendant with at least their names, dates of birth, addresses, Social Security numbers, health insurance information, and medical information, all Personal Information.

36. Defendant stored that information unencrypted and in an internet accessible network at the time of the Data Breach. Plaintiffs and Class Members did so on the understanding that Defendant would implement expected, promised, and reasonable data security safeguards.

37. In March of 2023 a relatively new threat actor calling itself Money Message began to target large companies that maintain sensitive employee or consumer information.

38. Money Message employs a "double extortion" technique in which it both steals sensitive data from the target's network and encrypts it so that the target can no longer use the data itself.[9] Money Message maintains its own "leak site" where it posts the stolen data if a ransom is not paid.[10]

39. Digital experts have noted that Money Message's techniques "do not appear sophisticated."[11] In analyzing Money Message's attacks, analysts have found that they were propagated by gaining access to an organization's network when administrative accounts were only protected by "single-factor authentication" – wherein data is protected by only a single credential, such as a password.[12] Experts, including the United States' Cybersecurity & Infrastructure Security Agency and Federal Communications Commission, recommend multifactor authentication for all applications, particularly where sensitive data is concerned.[13]

---

[9] https://cyble.com/blog/demystifying-money-message-ransomware/
[10] *Id*.
[11] https://www.bleepingcomputer.com/news/security/new-money-message-ransomware-demands-million-dollar-ransoms/
[12] https://www.scmagazine.com/native/step-by-step-through-the-money-message-ransomware
[13] *See, e.g.,* https://www.fcc.gov/protecting-your-personal-data; https://www.cisa.gov/resources-

40. Still, in their short time of operation, Money Message has successfully targeted and extracted Personal Information from large companies including a global PC parts manufacturer Micro-Star International or MSI, and Biman Airlines, a Bangladeshi airline with annual revenues exceeding $1-billion.

41. On March 28, 2023, Money Message claimed responsibility for the Data Breach and posted a sample of the patient information they had exfiltrated from PharMerica, including "a patient-related table with name, SSN, date of birth, Medicaid number, and Medicare number, [] an Excel file with [] name, date of birth, SSN, Medicaid Number, Medicare Number, allergies, and a field with somewhat detailed diagnoses information and history."[14] Security researchers subsequently verified that the information publicly posted by Money Message included unredacted and legitimate Social Security numbers and medical information belonging to identifiable individuals.

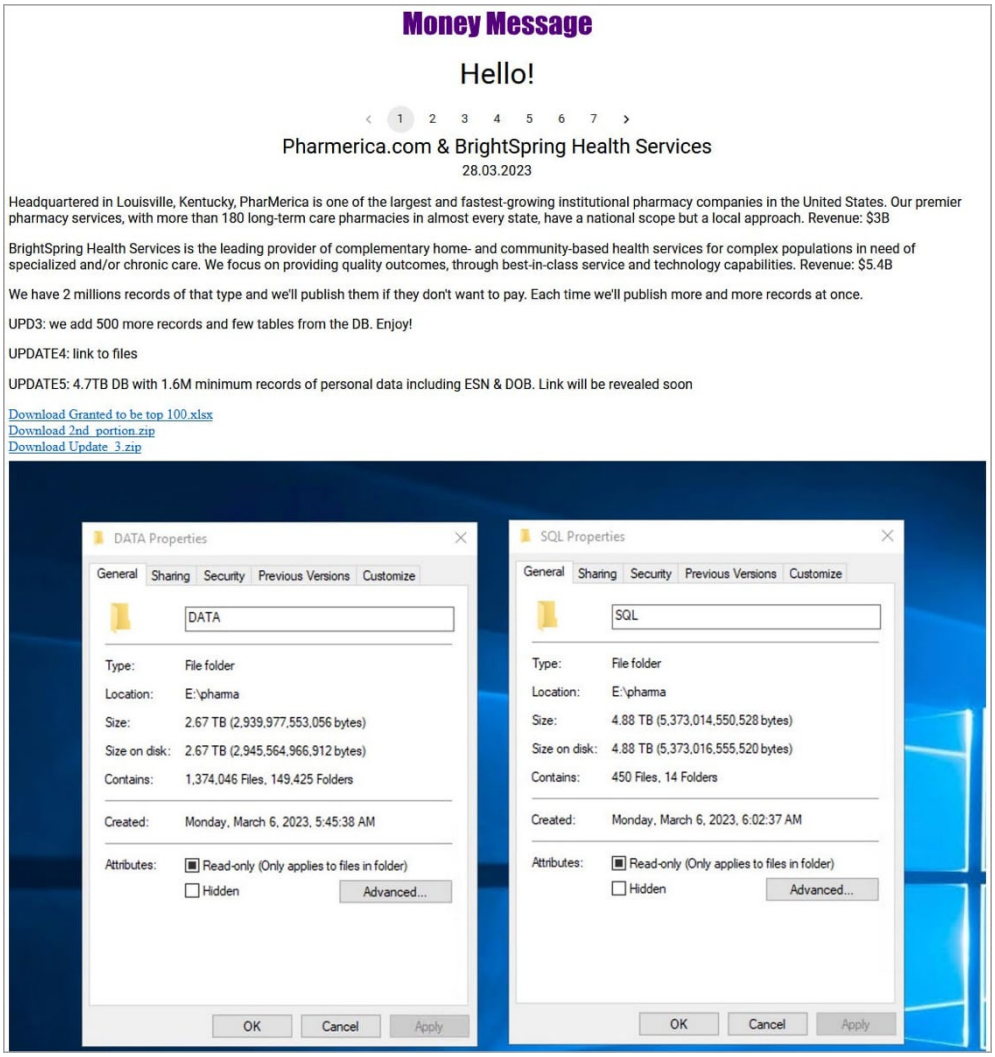
42. In April of 2023 Money Message posted yet another data dump of Personal Information and warned PharMerica that "[w]e have 2 millions [sic] records of that type and we'll publish them if they don't want to pay. Each time we'll publish more and more records at once"[15]:

---

tools/resources/multi-factor-authentication-mfa#:~:text=MFA%20increases%20security%20because%20even,device%2C%20network%2C%20or%20database.

[14] https://www.databreaches.net/pharmerica-and-brightspring-health-services-hit-by-money-message/

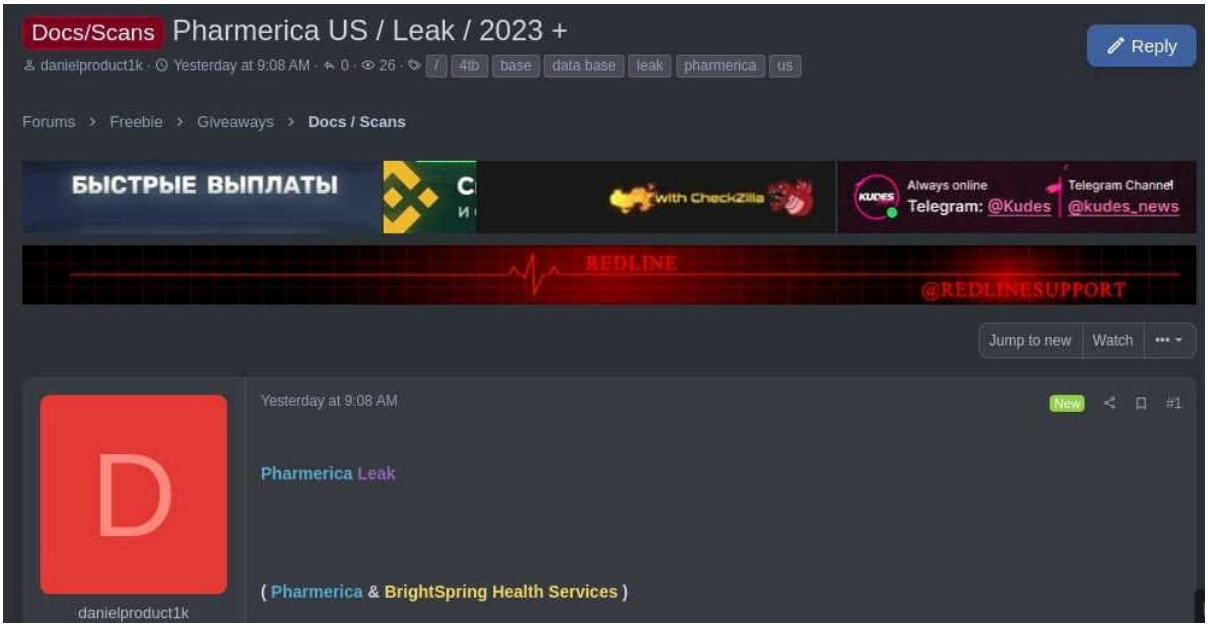
[15] https://www.bleepingcomputer.com/news/security/ransomware-gang-steals-data-of-58-million-pharmerica-patients/



43. In response to inquiries from cyber security researchers, Money Message provided samples of information stolen from PharMerica and belonging to patients of healthcare facilities in Alabama and North Carolina. The line items of those health records included:

> ID SSN PatientCode FirstName MI LastName County DOB MaritalStatus LevelOfService Birthplace Sex MedicaidNum MedicareNum OtherInsName OtherInsNum OtherInsGroupNum Comments Disabled PhysicianID AltPhysicianID DentistID DiagnosisID PharmacyID Payer Hospital EducationLevel FuneralHome RehabPotential Diagnosis DiagnosisText Prognosis Religion AdmittedFrom DatesOfStay1 DatesOfStay2 Nickname Race AmbulancePreference PreviousOccupation PatientAware NameOfChurch PharmacyMPS PharmacyOutside AdmissionNumber AllergiesText DiagnosesText TestPatient Notes.

44. Ultimately, Money Message made the entire database of patient information available on the dark web, splitting it into thirteen files for ease of download.[16] As of May 15, 2023, a month before PharMerica began informing Plaintiffs and Class Members of the Data Breach, their Personal Information was freely accessible and downloadable to anyone with an internet connection.[17]



45. In letters sent to Plaintiffs and Class Members nearly three months after PharMerica detected the Data Breach, and well after Money Message began publicly leaking the data that it stole, Defendant asserted that: "[o]n March 14, 2023, [Defendant] learned of suspicious activity on our computer network."[18] After launching an investigation, Defendant concluded—on an unspecified date—that "an unknown third party accessed [its] computer systems from March 12-13, 2023, and that certain personal information may have been obtained

[16] https://www.bleepingcomputer.com/news/security/ransomware-gang-steals-data-of-58-million-pharmerica-patients/
[17] *Id.*
[18] The "Notice Letter". A sample copy is available at https://apps.web.maine.gov/online/aeviewer/ME/40/08d6080b-afcf-4d02-ba20-24f639aaca61.shtml

from [its] systems as a part of the incident." Defendant's Notice Letter further shifted the burden to Plaintiffs and Class Members to "remain vigilant to protect against potential fraud and/or identity theft by, among other things, reviewing your account statements and monitoring credit reports closely." [19]

46. Omitted from PharMerica's Notice Letter were the root cause of the Data Breach, the vulnerabilities in PharMerica's systems that were exploited, and the remedial measures undertaken to ensure such a breach does not occur again. PharMerica also described the medical information and other PHI it allowed to be exfiltrated from its system in general terms while the information made available by Money Message includes detailed health records. Moreover, the Notice Letter made no mention that a known criminal group had already begun publicly posting the Personal Information that they exfiltrated during the Data Breach. To date, these omitted details have not been explained or clarified to Plaintiffs and Class Members, who retain a vested and ongoing need to ensure that their Personal Information remains protected from further access, disclosure, and misuse.

47. Money Message targeted Defendant due to its status as a healthcare entity that collects, creates, and maintains Personal Information on its computer networks and/or systems. The files containing Plaintiffs' and Class Members' Personal Information, that Defendant allowed to be accessed and exfiltrated from its systems, included at least their names, dates of birth, addresses, Social Security numbers, detailed medical histories, health insurance information, and medication information.[20]

48. As evidenced by the samples of Personal Information that Money Message has

[19] *Id.*
[20] *Id.*

publicly posted, the Personal Information contained in Defendant's network was not encrypted. Had the information been properly encrypted, Money Message would have exfiltrated only unintelligible data.[21]

49. Plaintiffs' Personal Information was targeted, accessed, and stolen in the Data Breach and their stolen Personal Information is currently publicly available for anyone wishing to download it from the internet.

50. Due to the present and continuing risk of identity theft as a result of the Data Breach, Plaintiffs and Class Members must, as Defendant's Notice Letter foists on them to do, "remain vigilant" and monitor their financial accounts for many years to mitigate the boundless risk of identity theft and future threat of harm brought on by the Data Breach.[22]

51. In the Notice Letter, Defendant offers 12 months of identity monitoring services. This is wholly inadequate to compensate Plaintiffs and Class Members because it fails to provide for the fact that victims of data breaches and other unauthorized disclosures commonly face multiple years of ongoing identity theft, medical and financial fraud, and it entirely fails to provide sufficient compensation for the unauthorized release and disclosure of Plaintiffs' and Class Members' Personal Information.

52. Defendant had obligations created by the FTC Act, HIPAA, contract, state and federal law, common law, and industry standards to keep Plaintiffs' and Class Members' Personal Information confidential and to protect it from unauthorized access and disclosure.

B. Data Breaches Are Preventable

[21] https://medium.com/@e.kozera/how-encryption-helps-protect-privacy-and-avoid-security-breaches-c82054c53920

[22] The "Notice Letter". A sample copy is available at https://apps.web.maine.gov/online/aeviewer/ME/40/08d6080b-afcf-4d02-ba20-24f639aaca61.shtml

53. A ransomware attack is a type of cyberattack frequently used to target healthcare providers due to the sensitive patient data they maintain.[23] In a ransomware attack the attackers use software to encrypt data on a compromised network, rendering it unusable and demanding payment to restore control over the network.[24] Ransomware attacks are particularly harmful for patients and healthcare providers alike as they cause operational disruptions that result in lengthier patient stays, delayed procedures or test results, increased complications from surgery, and even increased mortality rates.[25] In 2021, 44% of healthcare providers who experienced a ransomware attack saw their operations disrupted for up to a week and 25% experienced disrupted services for up to a month.[26]

54. Companies should treat ransomware attacks like any other data breach incident because ransomware attacks don't just hold networks hostage, "ransomware groups sell stolen data in cybercriminal forums and dark web marketplaces for additional revenue."[27] As cybersecurity expert Emisoft warns, "[a]n absence of evidence of exfiltration should not be construed to be evidence of its absence […] the initial assumption should be that data may have been exfiltrated."

55. An increasingly prevalent form of ransomware attack is the "encryption+exfiltration" attack in which the attacker encrypts a network and exfiltrates the data

---

[23] *Ransomware warning: Now attacks are stealing data as well as encrypting it*, available at https://www.zdnet.com/article/ransomware-warning-now-attacks-are-stealing-data-as-well-as-encrypting-it/

[24] *Ransomware FAQs*, available at https://www.cisa.gov/stopransomware/ransomware-faqs

[25] *Ponemon study finds link between ransomware, increased mortality rate*, available at https://www.healthcareitnews.com/news/ponemon-study-finds-link-between-ransomware-increased-mortality-rate

[26] *The State of Ransomware in Healthcare 2022*, available at https://assets.sophos.com/X24WTUEQ/at/4wxp262kpf84t3bxf32wrctm/sophos-state-of-ransomware-healthcare-2022-wp.pdf

[27] *Ransomware: The Data Exfiltration and Double Extortion Trends*, available at https://www.cisecurity.org/insights/blog/ransomware-the-data-exfiltration-and-double-extortion-trends

contained within.[28] In 2020, over 50% of ransomware attackers exfiltrated data from a network before encrypting it.[29] Once the data is exfiltrated from a network, its confidential nature is destroyed and it should be "assume[d] it will be traded to other threat actors, sold, or held for a second/future extortion attempt."[30] And even where companies pay for the return of data, attackers often leak or sell the data regardless because there is no way to verify copies of the data are destroyed.[31]

56. Defendant could have prevented this Data Breach by, among other things, properly encrypting or otherwise protecting their systems, equipment, and computer files containing Plaintiffs' and Class Members' Personal Information.

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

- Implemented an awareness and training program. Because end users are targets, patients and individuals should be aware of the threat of ransomware and how it is delivered.
- Enabled strong spam filters to prevent phishing emails from reaching the end users and authenticated inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.
- Scanned all incoming and outgoing emails to detect threats and filter executable files from reaching end users.
- Configured firewalls to block access to known malicious IP addresses.

---

[28] *The chance of data being stolen in a ransomware attack is greater than one in ten*, available at https://blog.emsisoft.com/en/36569/the-chance-of-data-being-stolen-in-a-ransomware-attack-is-greater-than-one-in-ten/

[29] 2020 Ransomware Marketplace Report, available at https://www.coveware.com/blog/q3-2020-ransomware-marketplace-report

[30] *Id*.

[31] *Id*.

- Patched operating systems, software, and firmware on devices, and considered using a centralized patch management system.
- Set anti-virus and anti-malware programs to conduct regular scans automatically.
- Managed the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.
- Configured access controls—including file, directory, and network share permissions—with least privilege in mind. If a user only needs to read specific files, the user should not have write access to those files, directories, or shares.
- Disabled macro scripts from office files transmitted via email. Considered using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.
- Implemented Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.
- Considered disabling Remote Desktop protocol (RDP) if it is not being used.
- Used application whitelisting, which only allows systems to execute programs known and permitted by security policy.
- Executed operating system environments or specific programs in a virtualized environment.
- Categorized data based on organizational value and implemented physical and logical separation of networks and data for different organizational units.[32]

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

Secure internet-facing assets

- Apply latest security updates

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

- Use threat and vulnerability management
- Perform regular audit; remove privileged credentials;

Thoroughly investigate and remediate alerts

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

Include IT Pros in security discussions

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

Build credential hygiene

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

Apply principle of least-privilege

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

Harden infrastructure

- Use Windows Defender Firewall
- Enable tamper protection
- Enable cloud-delivered protection
- Turn on attack surface reduction rules and [Antimalware Scan Interface] for Office[Visual Basic for Applications].[33]

59. Given that Defendant was storing the Personal Information of its current and former patients and employees, Defendant could and should have implemented all of the above measures to prevent and detect cyberattacks such as the Data Breach.

60. The occurrence of the Data Breach indicates that Defendant failed to adequately

[33] *See* Human-operated ransomware attacks: A preventable disaster (Mar 5, 2020), *available at:* https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/ (last visited Nov. 11, 2021).

implement one or more of the above measures, as well as other industry standard protections, to prevent cyberattacks, resulting in the Data Breach and, upon information and belief, the exposure of the Personal Information of nearly six million patients, including that of Plaintiffs and Class Members.

C. Defendant Knew or Should Have Known of the Risk Because Healthcare Entities In Possession Of Personal Information Are Particularly Suspectable To Cyber Attacks

61. Defendant's data security obligations were particularly important given the substantial increase in cyber-attacks and/or data breaches targeting healthcare entities that collect and store Personal Information, like Defendant, preceding the date of the Data Breach.

62. Data breaches, including those perpetrated against healthcare entities that store Personal Information in their systems, have become widespread.

63. Of the 1,862 recorded data breaches in 2021, 330 of them, or 17.7%, were in the medical or healthcare industry.[34]

64. The 330 healthcare breaches reported in 2021 exposed nearly 30 million sensitive records (28,045,658), compared to only 306 breaches that exposed nearly 10 million sensitive records (9,700,238) in 2020.[35]

65. Entities in custody of PHI and/or medical information reported the largest number of data breaches among all measured sectors in 2022, with the highest rate of exposure per breach.[36] Indeed, when compromised, healthcare related data is among the most sensitive and personally consequential. A report focusing on healthcare breaches found the "average total cost to resolve an identity theft-related incident . . . came to about $20,000," and that victims were

[34] *See id.* at n.15.
[35] *See id.*
[36] *See id.*, PageID.11 at n.17.

often forced to pay out of pocket costs for healthcare they did not receive in order to restore coverage.[37] Almost 50 percent of the victims lost their healthcare coverage as a result of the incident, while nearly 30 percent said their insurance premiums went up after the event. Forty percent of the patients were never able to resolve their identity theft at all. Data breaches and identity theft have a crippling effect on individuals, and detrimentally impact the economy as a whole.[38]

66. Indeed, cyber-attacks, such as the one experienced by Defendant, have become so notorious that the Federal Bureau of Investigation ("FBI") and the U.S. Secret Service have issued a warning to potential targets so they are aware of, and prepared for, a potential attack. As one report explained, smaller entities that store Personal Information are "attractive to ransomware criminals…because they often have lesser IT defenses and a high incentive to regain access to their data quickly."[39]

67. In light of recent high profile cybersecurity incidents at other healthcare partner and provider companies, including American Medical Collection Agency (25 million patients, March 2019), University of Washington Medicine (974,000 patients, December 2018), Florida Orthopedic Institute (640,000 patients, July 2020), Wolverine Solutions Group (600,000 patients, September 2018), Oregon Department of Human Services (645,000 patients, March 2019), Elite Emergency Physicians (550,000 patients, June 2020), Magellan Health (365,000 patients, April

---

[37] *Id.* at n.18.
[38] *See id.*
[39] See, Ben Kochman, *FBI, Secret Service Warn Of Targeted Ransomware,* November 18, 2019, available at https://www.law360.com/consumerprotection/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware?nl_pk=3ed44a08-fcc2-4b6c-89f0-aa0155a8bb51&utm_source=newsletter&utm_medium=email&utm_campaign=consumerprotection (last accessed Jan. 11, 2024).

2020), and BJC Health System (286,876 patients, March 2020), Defendant knew or should have known that its electronic records would be targeted by cybercriminals.

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

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

70. As a result of the Data Breach Defendant permitted to occur by virtue of its inadequate data security, Plaintiffs and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their Personal Information.

71. The injuries to Plaintiffs and Class Members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for the protection of the Personal Information of Plaintiffs and Class Members.

72. The ramifications of Defendant's failure to keep secure the Personal Information of Plaintiffs and Class Members are long lasting and severe. Once Personal Information is stolen––particularly PHI—fraudulent use of that information and damage to victims may continue for years.

D. Value Of Personal Information

73. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[40] 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."[41]

74. The PII of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web. The link between a data breach and the risk of identity theft is simple and well established. Criminals acquire and steal PII to monetize the information. Criminals monetize the data by selling the stolen information on the black market to other criminals who then utilize the information to commit a variety of identity theft related crimes discussed below.

75. Identity thieves use stolen PII such as Social Security numbers for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud. Identity thieves can also use Social Security numbers to obtain a driver's license or official identification card in the victim's name but with the thief's picture; use the victim's name and Social Security number to obtain government benefits; or file a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's Social Security number, rent a house or receive medical services in the victim's name, and may even give the victim's personal information to police during an arrest resulting in an arrest warrant being issued

[40] 17 C.F.R. § 248.201 (2013).
[41] *Id.*

in the victim's name.

76. Numerous sources cite dark web pricing for stolen identity credentials.[42] For example, Personal Information can be sold at a price ranging from $40 to $200.[43] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[44]

77. For example, the Social Security Administration has warned that identity thieves can use an individual's Social Security number to apply for additional credit lines.[45] Such fraud may go undetected until debt collection calls commence months, or even years, later. Stolen Social Security Numbers also make it possible for thieves to file fraudulent tax returns, file for unemployment benefits, or apply for a job using a false identity.[46] Each of these fraudulent activities is difficult to detect. An individual may not know that his or her Social Security Number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

78. Moreover, it is not an easy task to change or cancel a stolen Social Security number:

> An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. Even then, a new Social Security number may not be effective, as "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new

---

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

[43] *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, *available at*: https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/

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

[45] *Identity Theft and Your Social Security Number*, Social Security Administration (2018). Available at https://www.ssa.gov/pubs/EN-05-10064.pdf

[46] *Id*.

Social Security number."[47]

79. Theft of PHI is also gravely serious: "[a] thief may use your name or health insurance numbers to see a doctor, get prescription drugs, file claims with your insurance provider, or get other care. If the thief's health information is mixed with yours, your treatment, insurance and payment records, and credit report may be affected."[48]

80. Drug manufacturers, medical device manufacturers, pharmacies, hospitals, and other healthcare service providers often purchase PII and PHI on the black market for the purpose of target marketing their products and services to the physical maladies of the data breach victims themselves. Insurance companies purchase and use wrongfully disclosed PHI to adjust their insureds' medical insurance premiums.

81. Patient health records can sell for as much as $363 per record according to the Infosec Institute.[49] Medical information is particularly valuable because criminals can use it to target victims with frauds and scams. Indeed, "[o]ne reason medical data is coveted by thieves is that it has more lasting value than other types of information. Once the bad guys get their hands on it, it's difficult for the victim to do anything to protect themselves. While a stolen credit card can be cancelled and fraudulent charges disputed, the process for resolving medical ID theft is not as straightforward."[50]

82. Medicare numbers, like those that Money Message publicly posted following the

---

[47] Brian Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft

[48] *See* Federal Trade Commission, What to Know About Medical Identity Theft, https://www.consumer.ftc.gov/articles/what-know-about-medical-identity-theft identity-theft (last visited Jan. 25, 2022).

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

[50] *Id*.

Data Breach, have been offered for sale for as much as $470 per number.[51]

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

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[52]

84. This data, as one would expect, demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "[c]ompared to credit card information, personally identifiable information and Social Security Numbers are worth more than 10x on the black market."[53]

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

E. Defendant Fails To Comply With FTC Guidelines

86. The FTC has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need

---

[51] *Id*.

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

[53] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, Computer World (Feb. 6, 2015), http://www.itworld.com/article/2880960/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html

for data security should be factored into all business decision-making.

87. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cyber-security guidelines for businesses. These guidelines note that businesses should protect the personal patient information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.[54]

88. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[55]

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

90. The FTC has brought enforcement actions against healthcare entities for failing to protect patient data adequately and reasonably, 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 Federal Trade Commission Act ("FTCA"),

[54] *Protecting Personal Information: A Guide for Business*, Federal Trade Commission (2016). Available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf

[55] *Id.*

15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

91. These FTC enforcement actions include actions against healthcare providers like Defendant. *See, e.g., In the Matter of LabMd, Inc., A Corp*, 2016-2 Trade Cas. (PharMerica) ¶ 79708, 2016 WL 4128215, at *32 (MSNET July 28, 2016) ("[T]he Commission concludes that LabMD's data security practices were unreasonable and constitute an unfair act or practice in violation of Section 5 of the FTC Act.").

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

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

94. Upon information and belief, Defendant was at all times fully aware of its obligation to protect the Personal Information of its patients and employees. Defendant was also aware of the significant repercussions that would result from its failure to do so.

F. Defendant Fails To Comply With HIPAA Guidelines

95. Defendant is a covered entity under HIPAA (45 C.F.R. § 160.102) and is required to comply with the HIPAA Privacy Rule and Security Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and E ("Standards for Privacy of Individually Identifiable Health Information"), and Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C.

96. Defendant is subject to the rules and regulations for safeguarding electronic forms of medical information pursuant to the Health Information Technology Act ("HITECH").[56] *See*

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

42 U.S.C. §17921, 45 C.F.R. § 160.103.

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

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

99. 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.

100. "Electronic protected health information" is "individually identifiable health information … that is (i) transmitted by electronic media; maintained in electronic media." 45 C.F.R. § 160.103.

101. HIPAA's Security Rule requires Defendant to do the following:

a. Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits;

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

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

d. Ensure compliance by its workforce.

102. HIPAA also requires Defendant to "review and modify the security measures implemented … as needed to continue provision of reasonable and appropriate protection of

electronic protected health information." 45 C.F.R. § 164.306(e). Additionally, Defendant is required under HIPAA to "[i]mplement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights." 45 C.F.R. § 164.312(a)(1).

103. HIPAA and HITECH also obligated Defendant to implement policies and procedures to prevent, detect, contain, and correct security violations, and to protect against uses or disclosures of electronic protected health information that are reasonably anticipated but not permitted by the privacy rules. *See* 45 C.F.R. § 164.306(a)(1) and § 164.306(a)(3); *see also* 42 U.S.C. §17902.

104. The HIPAA Breach Notification Rule, 45 C.F.R. §§ 164.400-414, also requires Defendant to provide notice of the Data Breach to each affected individual "without unreasonable delay and ***in no case later than 60 days following discovery of the breach***."[57]

105. A Data Breach such as the one Defendant experienced is also considered a breach under the HIPAA Rules because there is an access of PHI not permitted under the HIPAA Privacy Rule:

> A breach under the HIPAA Rules is defined as, "...the acquisition, access, use, or disclosure of PHI in a manner not permitted under the [HIPAA Privacy Rule] which compromises the security or privacy of the PHI." See 45 C.F.R. 164.40

106. Data breaches are also Security Incidents under HIPAA because they impair both the integrity (data is not interpretable) and availability (data is not accessible) of patient health information:

> The presence of ransomware (or any malware) on a covered entity's or business

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

> associate's computer systems is a security incident under the HIPAA Security Rule. A security incident is defined as the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system. See the definition of security incident at 45 C.F.R. 164.304. Once the ransomware is detected, the covered entity or business associate must initiate its security incident and response and reporting procedures. See 45 C.F.R.164.308(a)(6).[58]

107. HIPAA requires a covered entity to have and apply appropriate sanctions against members of its workforce who fail to comply with the privacy policies and procedures of the covered entity or the requirements of 45 C.F.R. Part 164, Subparts D or E. *See* 45 C.F.R. § 164.530(e).

108. HIPAA requires a covered entity to mitigate, to the extent practicable, any harmful effect that is known to the covered entity of a use or disclosure of protected health information in violation of its policies and procedures or the requirements of 45 C.F.R. Part 164, Subpart E by the covered entity or its business associate. *See* 45 C.F.R. § 164.530(f).

109. HIPAA also requires the Office of Civil Rights ("OCR"), within the Department of Health and Human Services ("HHS"), to issue annual guidance documents on the provisions in the HIPAA Security Rule. *See* 45 C.F.R. §§ 164.302-164.318. For example, "HHS has developed guidance and tools to assist HIPAA covered entities in identifying and implementing the most cost effective and appropriate administrative, physical, and technical safeguards to protect the confidentiality, integrity, and availability of e-PHI and comply with the risk analysis requirements of the Security Rule." US Department of Health & Human Services, Security Rule Guidance Material.[59] The list of resources includes a link to guidelines set by the National Institute of Standards and Technology (NIST), which OCR says "represent the industry standard for good business practices with respect to standards for securing e-PHI." US Department of

[58] *See* https://www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf at 4.
[59] http://www.hhs.gov/hipaa/for-professionals/security/guidance/index.html.

Health & Human Services, Guidance on Risk Analysis.[60]

G. Defendant Fails To Comply With Industry Standards

110. As noted above, experts studying cyber security routinely identify entities in possession of Personal Information as being particularly vulnerable to cyberattacks because of the value of the Personal Information which they collect and maintain.

111. Several best practices have been identified that, at a minimum, should be implemented by healthcare entities in possession of Personal Information, like Defendant, including but not limited to: educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data and limiting which employees can access sensitive data. Defendant failed to follow these industry best practices, including a failure to implement multi-factor authentication.

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

113. Defendant failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center

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

for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

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

H. Common Injuries and Damages

115. As a result of Defendant's ineffective and inadequate data security practices, the Data Breach, and the foreseeable consequences of Personal Information ending up in the possession of criminals, the risk of identity theft to the Plaintiffs and Class Members has materialized and is imminent, and Plaintiffs and Class Members have all sustained actual injuries and damages, including: (a) invasion of privacy; (b) identity theft and fraud; (c) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft risk; (d) the loss of benefit of the bargain (price premium damages); (e) diminution of value of their Personal Information; (f) invasion of privacy; and (g) the continued risk to their Personal Information, which remains in the possession of Defendant, and which is subject to further breaches, so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiffs' and Class Members' Personal Information.

The Data Breach Increases Victims' Risk Of Identity Theft

116. Further, as a result of the Data Breach PharMerica permitted to occur, Plaintiffs and Class Members are at a heightened risk of identity theft for years to come.

117. The unencrypted Personal Information of Class Members will end up for sale on the dark web because that is the *modus operandi* of hackers. In addition, unencrypted Personal

Information may fall into the hands of companies that will use the detailed Personal Information for targeted marketing without the approval of Plaintiffs and Class Members. As a result of the Data Breach, unauthorized individuals can now easily access the Personal Information of Plaintiffs and Class Members.

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

119. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate and trick individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails. Data Breaches can be the starting point for these additional targeted attacks on the victim.

120. One such example of criminals piecing together bits and pieces of compromised Personal Information for profit is the development of "Fullz" packages.[61] With "Fullz" packages,

[61] "Fullz" is fraudster speak for data that includes the information of the victim, including, but not limited to, the name, address, credit card information, social security number, date of birth, and more. As a rule of thumb, the more information you have on a victim, the more money that can be made off of those credentials. Fullz are usually pricier than standard credit card credentials, commanding up to $100 per record (or more) on the dark web. Fullz can be cashed out (turning credentials into money) in various ways, including performing bank transactions over the phone with the required authentication details in-hand. Even "dead Fullz," which are Fullz credentials associated with credit cards that are no longer valid, can still be used for numerous purposes, including tax refund scams, ordering credit cards on behalf of the victim, or opening a "mule account" (an account that will accept a fraudulent money transfer from a compromised account)

cyber-criminals can cross-reference two sources of Personal Information to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals.

121. The development of "Fullz" packages means here that the stolen Personal Information from the Data Breach can easily be used to link and identify it to Plaintiffs' and Class Members' phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the Personal Information that was exfiltrated in the Data Breach, criminals may still easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over.

122. The existence and prevalence of "Fullz" packages means that the Personal Information stolen from the Data Breach can easily be linked to the unregulated data (like phone numbers and emails) of Plaintiff and the other Class Members.

123. Thus, even if certain information (such as emails or telephone numbers) was not stolen in the Data Breach, criminals can still easily create a comprehensive "Fullz" package.

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

Loss Of Time To Mitigate Risk Of Identity Theft And Fraud

125. As a result of the recognized risk of identity theft, when a data breach occurs, and an individual is notified by a company that their Personal Information was compromised, as in

---

without the victim's knowledge. *See*, *e.g.*, Brian Krebs, *Medical Records for Sale in Underground Stolen From Texas Life Insurance Firm*, Krebs on Security (Sep. 18, 2014), https://krebsonsecuritv.eom/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-](https://krebsonsecuritv.eom/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-finn/ (last visited on May 26, 2023).

this Data Breach, the reasonable person is expected to take steps and spend time to address the dangerous situation, learn about the breach, and otherwise mitigate the risk of becoming a victim of identity theft of fraud. Failure to spend time taking steps to review accounts or credit reports could expose the individual to greater financial harm – yet, the resource and asset of time has been lost.

126. Thus, due to the actual and imminent risk of identity theft, Plaintiffs and Class Members must, as Defendant's Notice Letter encourages them to do, "remain vigilant to protect against potential fraud and/or identity theft by, among other things, reviewing your account statements and monitoring credit reports closely."

127. Plaintiffs and Class Members have spent, and will spend additional time in the future, on a variety of prudent actions, such as researching and verifying the legitimacy of the Data Breach upon receiving the Notice Letter, checking if their information was exposed on the dark web, and checking their financial accounts for any indication of fraud, which may take years to detect.

128. Plaintiffs' mitigation efforts are consistent with the U.S. Government Accountability Office that released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[62]

129. Plaintiffs' mitigation efforts are also consistent with the steps that FTC recommends that data breach victims take several steps to protect their personal and financial information after a data breach, including: contacting one of the credit bureaus to place a fraud

[62] *See* United States Government Accountability Office, GAO-07-737, Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown (June 2007), https://www.gao.gov/new.items/d07737.pdf.

alert (consider an extended fraud alert that lasts for seven years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[63]

130. And for those Class Members who experience actual identity theft and fraud, the GAO Report notes that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[64]

Diminution Of Value Of Plaintiffs' and Class Members' Personal Information

131. PII and PHI are valuable property rights.[65] Their value is axiomatic, considering the value of Big Data in corporate America and the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that Personal Information has considerable market value.

132. An active and robust legitimate marketplace for Personal Information exists. In 2022, the data brokering industry was worth roughly $268 billion.[66] In fact, the data marketplace is so sophisticated that consumers can actually sell their non-public information directly to a data broker who in turn aggregates the information and provides it to marketers or app developers.[67,68] Consumers who agree to provide their web browsing history to the Nielsen Corporation can

---

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

[64] *See* "Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown," p. 2, U.S. Government Accountability Office, June 2007, https://www.gao.gov/new.items/d07737.pdf ("GAO Report").

[65] *See, e.g.,* Randall T. Soma, et al, Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("Personal Information") Equals the "Value" of Financial Assets, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) ("Personal Information, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

[66] https://www.maximizemarketresearch.com/market-report/global-data-broker-market/55670/

[67] https://datacoup.com/

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

receive up to $50.00 a year.[69]

133. Users of the personal data collection app Streamlytics can earn up to $200 a month by selling their Personal Information to marketing companies who use it to build consumer demographics profiles.[70]

134. Consumers also recognize the value of their Personal Information and offer it in exchange for goods and services. The value of Personal Information can be derived not by a price at which consumers themselves actually seek to sell it, but rather in the economic benefit consumers derive from being able to use it and control the use of it. For example, Plaintiffs and Class Members were only able to obtain services from Defendant after providing it with their Personal Information and their ability to use their Personal Information is encumbered when their identity or credit profile is infected by misuse or fraud. For example, a consumer with false or conflicting information on their credit report may be denied credit or be forced to pay a higher interest rate. Similarly, someone with false claims using their medical information can find difficulty receiving healthcare or managing their healthcare.

135. For instance, loss of access to patient histories, charts, images, and other information forces providers to limit or cancel patient treatment because of the disruption of service. This leads to a deterioration in the quality of overall care patients receive at facilities affected by data breaches. Researchers have found that among medical service providers that experience a data security incident, the death rate among patients increased in the months and

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

[70] How To Sell Your Own Data And Why You May Want to, available at https://www.mic.com/impact/selling-personal-data-streamlytics

years after the attack.[71] Researchers have further found that at medical service providers that experienced a data security incident, the incident was associated with deterioration in timeliness and patient outcomes, generally.[72]

136. Similarly, data breach incidents cause patients' issues with receiving care that rise above the level of mere inconvenience. The issues that patients encounter as a result of such incidents include, but are not limited to:

a. rescheduling their medical treatment;

b. finding alternative medical care and treatment;

c. delaying or foregoing medical care and treatment;

d. undergoing medical care and treatment without medical providers having access to a complete medical history and records; and

e. inability to access their medical records.

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

138. Based on the foregoing, the information compromised in the Data Breach is

[71] *See* Nsikan Akpan, Ransomware and Data Breaches Linked to Uptick in Fatal Heart Attacks, PBS (Oct. 24, 2019), https://www.pbs.org/newshour/science/ransomware-and-other-data-breaches-linked-to-uptick-in-fatal-heart- attacks (last visited Jan. 25, 2022).

[72] *See* Sung J. Choi et al., Cyberattack Remediation Efforts and Their Implications for Hospital Quality, 54 Health Services Research 971, 971-980 (2019). Available at https://onlinelibrary.wiley.com/doi/full/10.1111/1475-6773.13203 (last visited Jan. 25, 2022).

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

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

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

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[73]

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

142. Defendant was, or should have been, fully aware of the unique type and the significant volume of data on Defendant's network, amounting to nearly six million individuals' detailed personal information, upon information and belief, and thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

---

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

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

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

144. Given the type of targeted attack in this case and sophisticated criminal activity, the type of Personal Information involved, and the volume of data obtained in the Data Breach, there is a strong probability that entire batches of stolen information have been placed, or will be placed, on the black market/dark web for sale and purchase by criminals intending to utilize the Personal Information for identity theft crimes –e.g., opening bank accounts in the victims' names to make purchases or to launder money; file false tax returns; take out loans or lines of credit; or file false unemployment claims.

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

146. Furthermore, the information accessed and disseminated in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach, where victims can easily cancel or close credit and debit card accounts.[74] The information disclosed in this Data Breach is impossible to "close" and difficult, if not impossible, to change (such as Social Security numbers).

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

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

148. The retail cost of credit monitoring and identity theft monitoring can cost around $200 a year per Class Member. This is a reasonable and necessary cost to protect Class Members from the risk of identity theft that arose from Defendant's Data Breach. This is a future cost for a minimum of five years that Plaintiffs and Class Members would not need to bear but for Defendant's failure to safeguard their Personal Information.

Loss Of The Benefit Of The Bargain

149. Furthermore, Defendant's poor data security deprived Plaintiffs and Class Members of the benefit of their bargain. When agreeing to pay Defendant and/or its partners for the provision of medical services, Plaintiffs and other reasonable consumers understood and expected that they were, in part, paying for the service and necessary data security to protect the Personal Information, when in fact, Defendant did not provide the expected data security. Accordingly, Plaintiffs and Class Members received services that were of a lesser value than what they reasonably expected to receive under the bargains they struck with Defendant.

I. Plaintiffs' Experiences

Plaintiff David Hibbard

150. Plaintiff Hibbard was an employee from approximately 2014 to 2020 of ResCare, Inc., which changed its name to BrightSpring on August 15, 2018[75] before subsequently merging with PharMerica on approximately March 6, 2019.[76] On information and belief, Plaintiff Hibbard provided his Personal Information to BrightSpring, who in turn provided Plaintiff's information

[75] https://www.brightspringhealth.com/media-hub/kentucky-based-rescare-is-now-brightspring-health-services/
[76] https://www.brightspringhealth.com/media-hub/brightspring-pharmerica/

to Defendant, as a condition of working for BrightSpring. Defendant then entered Plaintiff's information into Defendant's computer system maintained by Defendant.

151. On or around August 11, 2023, Plaintiff Hibbard received a Notice letter from Defendant informing him that his Personal Information had been compromised in the Data Breach. The Notice letter stated that Plaintiff Hibbard's full name, address, date of birth, and Social Security number were accessed in the Data Breach.

152. Recognizing the present, immediate, and substantially increased risk of harm Plaintiff Hibbard faces, Defendant offered him a one-year subscription to a credit monitoring service. The Notice letter Plaintiff Hibbard received also cautioned him to "remain vigilant to protect against potential fraud and/or identity theft by, among other things, reviewing your account statements and monitoring credit reports closely."

153. Plaintiff Hibbard greatly values his privacy and Personal Information and takes reasonable steps to maintain the confidentiality of his Personal Information. Plaintiff Hibbard is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

154. Plaintiff Hibbard stores any and all documents containing Personal Information in a secure location and destroys any documents he receives in the mail that contain any Personal Information or that may contain any information that could otherwise be used to compromise his identity and credit card accounts. Moreover, he diligently chooses unique usernames and passwords for his various online accounts.

155. As a result of the Data Breach, Plaintiff Hibbard has spent time researching the Data Breach, verifying the legitimacy of the Notice letter, signing up for credit monitoring and identity theft monitoring service with Experian, reviewing his bank accounts, monitoring his

credit report, changing his passwords and payment account numbers, and other necessary mitigation efforts. This is valuable time that Plaintiff spent at Defendant's direction and that he otherwise would have spent on other activities, including but not limited to work and/or recreation.

156. As a consequence of and following the Data Breach, Plaintiff Hibbard has experienced an increase in spam and suspicious calls and texts messages. Furthermore, in July 2023, Plaintiff Hibbard came home to a package at his door containing a credit card issued by Verizon (Synchrony) in his name, that he never applied for. Thus, on information and belief, this credit card was applied for fraudulently in his name using Plaintiff's personal information compromised in the Data Breach. Plaintiff Hibbard contacted Verizon (Synchrony) to report this fraudulent conduct and was informed that the card had a balance of $208 in fraudulent charges. Plaintiff spent approximately 15 hours contacting Verizon (Synchrony) to dispute and troubleshoot this fraudulent conduct. Also, Plaintiff Hibbard was forced to contact Experian to have the fraudulent credit card account removed from his credit report and history, which Plaintiff Hibbard spend approximately 5 hours investigating, researching, and doing. Since experiencing this substantial fraudulent conduct, Plaintiff Hibbard has been forced to closely monitor his credit through CreditKarma, purchase Experian's Premium credit monitoring service (which costs $39.99 per month), and has contacted all three credit bureaus to freeze his credit multiple times. In total, Plaintiff Hibbard estimates that he has spent approximately 30-35 hours as a result of the Data Breach.

157. The Data Breach has caused Plaintiff Hibbard to suffer fear, anxiety, and stress, which has been compounded by Defendant's five-month delay in informing him of the fact that his Personal Information, including his Social Security number in conjunction with his date of

birth, was acquired by criminals as a result of the Data Breach.

158. Plaintiff Hibbard anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. In addition, Plaintiff Hibbard will continue to be at present and continued increased risk of identity theft and fraud for years to come.

159. Plaintiff Hibbard has a continuing interest in ensuring that his Personal Information, which upon information and belief, remains in Defendant's possession, is protected and safeguarded from future breaches.

Plaintiff Frank Raney

160. On information and belief, Plaintiff Raney received services from PharMerica while receiving post-operation care at a nursing home. On information and belief, Plaintiff Raney provided his Personal Information to the nursing home, who in turn provided Plaintiff's information to Defendant, as a condition of receiving services from Defendant. Defendant then entered Plaintiff's information into Defendant's computer system maintained by Defendant.

161. On or around June 9, 2023, Plaintiff Raney received a Notice letter from Defendant informing him that his Personal Information had been compromised in the Data Breach. The Notice letter stated that Plaintiff Raney's full name, address, date of birth, Social Security number, medications and health insurance information were accessed in the Data Breach.

162. Recognizing the present, immediate, and substantially increased risk of harm Plaintiff Raney faces, Defendant offered him a one-year subscription to a credit monitoring service. The Notice letter Plaintiff Raney received also cautioned him to "remain vigilant to protect against potential fraud and/or identity theft by, among other things, reviewing your

account statements and monitoring credit reports closely."

163. Plaintiff Raney greatly values his privacy and Personal Information and takes reasonable steps to maintain the confidentiality of his Personal Information. Plaintiff Raney is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

164. Plaintiff Raney stores any and all documents containing Personal Information in a secure location and destroys any documents he receives in the mail that contain any Personal Information or that may contain any information that could otherwise be used to compromise his identity and credit card accounts. Moreover, he diligently chooses unique usernames and passwords for his various online accounts.

165. As a result of the Data Breach, Plaintiff Raney has spent time researching the Data Breach, verifying the legitimacy of the Notice letter, signing up for the credit monitoring service, reviewing his bank accounts, monitoring his credit report, changing his passwords and payment account numbers, and other necessary mitigation efforts. This is valuable time that Plaintiff spent at Defendant's direction and that he otherwise would have spent on other activities, including but not limited to work and/or recreation.

166. As a consequence of and following the Data Breach, Plaintiff Raney has experienced an increase in spam and suspicious calls and texts messages.

167. The Data Breach has caused Plaintiff Raney to suffer fear, anxiety, and stress, which has been compounded by Defendant's two month delay in noticing him of the fact that his Personal Information, including his Social Security number in conjunction with his date of birth, was acquired by criminals as a result of the Data Breach.

168. Plaintiff Raney anticipates spending considerable time and money on an ongoing

basis to try to mitigate and address harms caused by the Data Breach. In addition, Plaintiff Raney will continue to be at present and continued increased risk of identity theft and fraud for years to come.

169. Plaintiff Raney has a continuing interest in ensuring that his Personal Information, which upon information and belief, remains in Defendant's possession, is protected and safeguarded from future breaches.

Plaintiff Holly Williams

170. Plaintiff Williams has no known relationship to PharMerica. Plaintiff Williams never consented to PharMerica collecting and storing her Personal Information.

171. On or around November 2023, Plaintiff Williams received a Notice letter from BrightSpring, a company that merged with PharMerica on approximately March 6, 2019,[77] informing her that her Personal Information had been compromised in the PharMerica Data Breach.[78] The Notice letter stated that Plaintiff Williams's full name, address, date of birth, and Social Security number, were accessed in the Data Breach.

172. Recognizing the present, immediate, and substantially increased risk of harm Plaintiff Williams faces, Defendant offered her a one-year subscription to a credit monitoring service.

173. Plaintiff Williams greatly values her privacy and Personal Information and takes reasonable steps to maintain the confidentiality of her Personal Information. Plaintiff Williams is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

[77] https://www.brightspringhealth.com/media-hub/brightspring-pharmerica/
[78] https://pharmerica.com/data-privacy-incident/

174. Plaintiff Williams stores any and all documents containing Personal Information in a secure location and destroys any documents she receives in the mail that contain any Personal Information or that may contain any information that could otherwise be used to compromise her identity and credit card accounts. Moreover, she diligently chooses unique usernames and passwords for her various online accounts.

175. As a result of the Data Breach, Plaintiff Williams has spent time researching the Data Breach, verifying the legitimacy of the Notice letter, signing up for the credit monitoring service, reviewing her bank accounts, monitoring her credit report, and other necessary mitigation efforts. This is valuable time that Plaintiff spent that she otherwise would have spent on other activities, including but not limited to work and/or recreation.

As a consequence of and following the Data Breach, Plaintiff Williams has received an increase in spam and suspicious calls and text messages.

176. The Data Breach has caused Plaintiff Williams to suffer fear, anxiety, and stress, which has been compounded by the eight-month delay in noticing her of the fact that her Personal Information, including her Social Security number in conjunction with her date of birth, was acquired by criminals as a result of the Data Breach.

177. Plaintiff Williams anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. In addition, Plaintiff Williams will continue to be at present and continued increased risk of identity theft and fraud for years to come.

178. Plaintiff Williams has a continuing interest in ensuring that her Personal Information, which upon information and belief, remains in Defendant's possession, is protected and safeguarded from future breaches.

Plaintiff James Young

179. Plaintiff Young has no known relationship to PharMerica. Plaintiff Young has never consented to PharMerica collecting and storing his Personal Information.

180. On or around June 14, 2023, Plaintiff Young received a Notice letter from Defendant informing him that his Personal Information had been compromised in the Data Breach. The Notice letter stated that Plaintiff Young's full name, address, date of birth, Social Security number, medications and health insurance information were accessed in the Data Breach.

181. Recognizing the present, immediate, and substantially increased risk of harm Plaintiff Young faces, Defendant offered him a one-year subscription to a credit monitoring service. The Notice letter Plaintiff Young received also cautioned him to "remain vigilant to protect against potential fraud and/or identity theft by, among other things, reviewing your account statements and monitoring credit reports closely."

182. Plaintiff Young greatly values his privacy and Personal Information and takes reasonable steps to maintain the confidentiality of his Personal Information. Plaintiff Young is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

183. Plaintiff Young stores any and all documents containing Personal Information in a secure location and destroys any documents he receives in the mail that contain any Personal Information or that may contain any information that could otherwise be used to compromise his identity and credit card accounts. Moreover, he diligently chooses unique usernames and passwords for his various online accounts.

184. To Plaintiff Young's knowledge, his Personal Information has not been

compromised in a prior data breach.

185. As a result of the Data Breach, Plaintiff Young has spent approximately 5 hours researching the Data Breach, verifying the legitimacy of the Notice letter, reviewing his accounts and balances, and other necessary mitigation efforts. This is valuable time that Plaintiff spent at Defendant's direction and that he otherwise would have spent on other activities, including but not limited to work and/or recreation.

186. The Data Breach has caused Plaintiff Young to suffer fear, anxiety, and stress, which has been compounded by Defendant's two-month delay in noticing him of the fact that his Personal Information, including his Social Security number in conjunction with his date of birth was acquired by criminals as a result of the Data Breach.

187. Plaintiff Young anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. In addition, Plaintiff Young will continue to be at present and continued increased risk of identity theft and fraud for years to come.

188. Plaintiff Young has a continuing interest in ensuring that his Personal Information, which upon information and belief, remains in Defendant's possession, is protected and safeguarded from future breaches.

Plaintiff Micaela Molina

189. From approximately September 2021 until March 29, 2023, Plaintiff Molina was employed at BrightSpring, a company that merged with PharMerica on approximately March 6, 2019.[79]

190. As a condition of employment, Ms. Molina was required to provide her Personal

[79] https://www.brightspringhealth.com/media-hub/brightspring-pharmerica/

Information to BrightSpring and PharMerica, including at least her name and Social Security Number.

191. Ms. Molina provided her Personal Information and trusted that BrightSpring and PharMerica would use reasonable measures to protect it according to state and federal law.

192. On or around June 30, 2023, Plaintiff Molina received a Notice letter informing her that her Personal Information had been compromised in the PharMerica Data Breach.[80] The Notice letter stated that Plaintiff Molina's full name and Social Security number, were accessed in the Data Breach.

193. Recognizing the present, immediate, and substantially increased risk of harm Plaintiff Molina faces, Defendant offered her one-year subscription to a credit monitoring service.

194. Plaintiff Molina greatly values her privacy and Personal Information and takes reasonable steps to maintain the confidentiality of her Personal Information. Plaintiff Molina is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

195. Plaintiff Molina stores any and all documents containing Personal Information in a secure location and destroys any documents she receives in the mail that contain any Personal Information or that may contain any information that could otherwise be used to compromise her identity and credit card accounts. Moreover, she diligently chooses unique usernames and passwords for her various online accounts.

196. As a result of the Data Breach, Plaintiff Molina has spent time researching the Data Breach, verifying the legitimacy of the Notice letter, signing up for the credit monitoring service, reviewing her bank accounts, monitoring her credit report, and other necessary mitigation

[80] https://pharmerica.com/data-privacy-incident/

efforts. This is valuable time that Plaintiff spent at Defendant's direction and that she otherwise would have spent on other activities, including but not limited to work and/or recreation.

197. As a consequence of and following the Data Breach, Plaintiff Molina has received an increase in spam and suspicious calls and text messages.

198. The Data Breach has caused Plaintiff Molina to suffer fear, anxiety, and stress, which has been compounded by Defendant's three-month delay in noticing her of the fact that her Personal Information, including her Social Security number in conjunction with her date of birth was acquired by criminals as a result of the Data Breach.

199. Plaintiff Molina anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. In addition, Plaintiff will continue to be at present and continued increased risk of identity theft and fraud for years to come.

Plaintiff Molina has a continuing interest in ensuring that her Personal Information, which upon information and belief, remains in Defendant's possession, is protected and safeguarded from future breaches.

Plaintiff Charley Luther

200. Plaintiff Luther never provided her Personal Information, PII or PHI, to PharMerica directly. On information and belief, Plaintiff Luther's name, address, date of birth, Social Security number, medications, and health insurance information were provided to her medical providers at various times when she obtained health services and those were provided to Pharmerica.

201. Plaintiff Luther received a Notice letter informing her that her PII and PHI had

been compromised in the PharMerica Data Breach.[81]

202. Recognizing the present, immediate, and substantially increased risk of harm Plaintiff Luther faces, Defendant offered her one-year subscription to a credit monitoring service.

203. Plaintiff Luther greatly values her privacy and PII and PHI and takes reasonable steps to maintain the confidentiality of her Personal Information. Plaintiff Luther is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

204. Plaintiff Luther stores any and all documents containing PII and PHI in a safe and secure location and destroys any documents she receives in the mail that contain any PII or PHI or that may contain any information that could otherwise be used to compromise her identity and credit card accounts. Moreover, she diligently chooses unique usernames and passwords for her various online accounts.

205. As a result of the Data Breach, Plaintiff Luther has spent money and time researching the Data Breach, verifying the legitimacy of the Notice letter, signing up for a credit monitoring service, reviewing her bank accounts, monitoring her credit report, and other necessary mitigation efforts. This is valuable time that Plaintiff spent at Defendant's direction and that she otherwise would have spent on other activities, including but not limited to work and/or recreation.

206. As a consequence of and following the Data Breach, Plaintiff Luther has received an increase in spam and suspicious calls and text messages.

207. Following the PharMerica Data Breach, Plaintiff Luther received three suspicious calls from someone posing as a representative of her bank. The caller had PII about her.

[81] https://pharmerica.com/data-privacy-incident/

208. Plaintiff Luther spent several hours addressing the attempted fraud and had her debit card reissued and one of her bank accounts closed.

209. The Data Breach has caused Plaintiff Luther to suffer fear, anxiety, and stress, which has been compounded by Defendant's three-month delay in noticing her that her Personal Information, was compromised in the Data Breach.

210. Plaintiff Luther anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. In addition, Plaintiff Luther will continue to be at present and continued increased risk of identity theft and fraud for years to come.

211. Plaintiff Luther has a continuing interest in ensuring that her PII and PHI, which upon information and belief, remains in Defendant's possession, is protected and safeguarded from future breaches.

CLASS ACTION ALLEGATIONS

212. This action is properly maintainable as a class action. Plaintiffs bring this class action on behalf of themselves, and on behalf of all others similarly situated.

213. Plaintiffs seek to certify the following classes, subject to amendment as appropriate:

Nationwide Class: All individuals residing in the United States whose Personal Information was compromised in the Data Breach, including all those who received a Notice Letter (the "Class").

Kentucky Subclass: All individuals residing in the Commonwealth of Kentucky whose Personal Information was compromised in the Data Breach, including all those who received a Notice Letter.

California Subclass: All individuals residing in the State of California whose Personal Information was compromised in the Data Breach, including all those who received a Notice Letter.

Michigan Subclass: All individuals residing in the State of Michigan whose Personal Information was compromised in the Data Breach, including all those who received a Notice Letter.

Texas Subclass: All individuals residing in the State of Texas whose Personal Information was compromised in the Data Breach, including all those who received a Notice Letter.

South Carolina Subclass: All individuals residing in the State of South Carolina whose Personal Information was compromised in the Data Breach, including all those who received a Notice Letter.

214. The Kentucky, California, Michigan, Texas, and South Carolina Subclasses are collectively referred to as the "State Subclasses" and together with the Nationwide Class, the "Class." Excluded from the Class are the following individuals and/or entities: Defendant and Defendant's parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendant has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

215. Numerosity: The members of the Class are so numerous that joinder of all members is impracticable, if not completely impossible. At least 5,800,000 individuals were notified by Defendant of the Data Breach, according to the breach report submitted to Maine's Attorney General's Office.[82] The Class is apparently identifiable within Defendant's records, and Defendant has already identified these individuals (as evidenced by sending them breach notification letters).

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

a. Whether and to what extent Defendant had a duty to protect the Personal Information of Plaintiffs and Class Members;

[82] https://apps.web.maine.gov/online/aeviewer/ME/40/08d6080b-afcf-4d02-ba20-24f639aaca61.shtml (last visited July 3, 2023).

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

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

d. Whether Defendant failed to adequately safeguard the Personal Information of Plaintiffs and Class Members;

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

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

g.. Whether Defendant violated the law by failing to promptly notify Plaintiffs and Class Members that their Personal Information had been compromised;

h. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

i. Whether Defendant adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

j. Whether Plaintiffs and Class Members are entitled to actual damages, statutory damages, and/or nominal damages as a result of Defendant's wrongful conduct; and

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

217. Typicality: Plaintiffs' claims are typical of those of the other members of the Class because Plaintiffs, like every other Class Member, was exposed to virtually identical conduct in

their Personal Information being compromised in the Data Breach permitted to occur by Defendant, and now suffers from the same violations of the duties of care and the law as each other member of the Class.

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

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

220. Superiority and Manageability: The class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of Class Members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain Class Members, who could not individually

afford to litigate a complex claim against large corporations, like Defendant. Further, even for those Class Members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

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

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

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

224. Unless a Class-wide injunction is issued, Defendant may continue in its failure to properly secure the Personal Information of Class Members, Defendant may continue to refuse to provide proper notification to Class Members regarding the Data Breach, and Defendant may continue to act unlawfully as set forth in this Complaint.

225. Further, Defendant has acted or refused to act on grounds generally applicable to the Class and, accordingly, final injunctive or corresponding declaratory relief with regard to the Class Members as a whole is appropriate under Code of Civil Procedure § 382.

COUNT I
NEGLIGENCE
(On Behalf of Plaintiffs and the Nationwide Class or, in the Alternative, the State Subclasses)

226. Plaintiffs restate and reallege the preceding factual allegations set forth above as if fully alleged herein.

227. Defendant requires its patients, employees, and patients of its healthcare partners, including Plaintiffs and Class Members, to submit non-public Personal Information in the ordinary course of providing its medical services.

228. Defendant gathered and stored the Personal Information of Plaintiffs and Class Members in its information technology computer systems as part of its business of soliciting its services to its clients and its clients' patients, which solicitations and services affect commerce.

229. Plaintiffs and Class Members entrusted Defendant with their Personal Information, whether directly or indirectly, with the understanding that Defendant would safeguard their information.

230. Defendant had full knowledge of the sensitivity of the Personal Information and the types of harm that Plaintiffs and Class Members could and would suffer if the Personal Information were wrongfully disclosed.

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

and to safeguard the information from theft and compromise. Defendant's duty included a responsibility to implement processes by which they could detect a breach of its security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a data breach.

232. Defendant owed a duty of care to Plaintiff and Class Members because it was foreseeable that Defendant's failure to adequately safeguard their Personal Information in accordance with state-of-the-art industry standards concerning data security would result in the compromise of that Private Information—just like the Data Breach that ultimately came to pass.

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

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

235. For instance, HIPAA required Defendant to notify victims of the Breach within 60 days of the discovery of the Data Breach. Defendant did not begin to notify Plaintiffs or Class Members of the Data Breach until June 14, 2023, despite Defendant knowing on or about March 14, 2023, that unauthorized persons had accessed and acquired the private, protected, personal information of Plaintiffs and the Class.

236. Defendant owed a duty of care to Plaintiffs and Class Members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that its systems and networks, and the personnel responsible for them, adequately protected the Personal Information.

237. Defendant's duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendant and its patients. That special relationship arose because Plaintiffs and the Class entrusted Defendant with their confidential Personal Information, a necessary part of being patients of Defendant.

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

239. Defendant was subject to an "independent duty," untethered to any contract between Defendant and Plaintiffs or the Class.

240. Defendant also had a duty to exercise appropriate clearinghouse practices to remove former patients' Personal Information it was no longer required to retain pursuant to regulations.

241. Moreover, Defendant had a duty to promptly and adequately notify Plaintiffs and the Class of the Data Breach.

242. Defendant had and continues to have a duty to adequately disclose that the Personal Information of Plaintiffs and the Class within Defendant's possession might have been compromised, how it was compromised, and precisely the types of data that were compromised and when. Such notice was necessary to allow Plaintiffs and the Class to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their Personal Information by third parties.

243. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' Personal Information;

b. Failing to adequately monitor the security of their networks and systems;

c. Failure to periodically ensure that their email system had plans in place to maintain reasonable data security safeguards;

d. Allowing unauthorized access to Class Members' Personal Information;

e. Failing to detect in a timely manner that Class Members' Personal Information had been compromised;

f. Failing to remove former patients' Personal Information when it was no longer required to retain pursuant to regulations,

g. Failing to timely and adequately notify Class Members about the Data Breach's occurrence and scope, so that they could take appropriate steps to mitigate the potential for identity theft and other damages; and

h. Failing to secure its stand-alone personal computers, such as the reception desk computers, even after discovery of the data breach.

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

245. It was foreseeable that Defendant's failure to use reasonable measures to protect Class Members' Personal Information would result in injury to Class Members. Further, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data

breaches in the healthcare industry.

246. Defendant has full knowledge of the sensitivity of the Personal Information and the types of harm that Plaintiffs and the Class could and would suffer if the Personal Information were wrongfully disclosed.

247. Plaintiffs and the Class were the foreseeable and probable victims of any inadequate security practices and procedures. Defendant knew or should have known of the inherent risks in collecting and storing the Personal Information of Plaintiffs and the Class, the critical importance of providing adequate security of that Personal Information, and the necessity for encrypting Personal Information stored on Defendant's systems.

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

249. Plaintiffs and the Class had no ability to protect their Personal Information that was in, and possibly remains in, Defendant's possession.

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

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

252. Defendant has admitted that the Personal Information of Plaintiffs and the Class was wrongfully lost and disclosed to unauthorized third persons as a result of the Data Breach.

253. But for Defendant's wrongful and negligent breach of duties owed to Plaintiffs and the Class, the Personal Information of Plaintiffs and the Class would not have been compromised.

254. There is a close causal connection between Defendant's failure to implement security measures to protect the Personal Information of Plaintiffs and the Class and the harm, or risk of imminent harm, suffered by Plaintiffs and the Class. The Personal Information of Plaintiffs and the Class was lost and accessed as the proximate result of Defendant's failure to exercise reasonable care in safeguarding such Personal Information by adopting, implementing, and maintaining appropriate security measures.

255. As a direct and proximate result of Defendant's negligence, Plaintiffs and the Class have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to invasion of privacy; theft of and fraudulent use of their Personal Information; lost or diminished value of Personal Information; lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; loss of benefit of the bargain; lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; experiencing an increase in spam calls, texts, and/or emails; dissemination of the Personal Information on the dark web; statutory damages; nominal damages; and anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

256. Additionally, as a direct and proximate result of Defendant's negligence, Plaintiffs and the Class have suffered and will suffer the continued risks of exposure of their Personal Information, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Personal Information in its continued possession.

257. Plaintiffs and Class Members are entitled to compensatory and consequential

damages suffered as a result of the Data Breach.

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

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

COUNT II
BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiffs and the Nationwide Class or, in the Alternative, the State Subclasses)

260. Plaintiffs restate and reallege the preceding factual allegations set forth above as if fully alleged herein.

261. This count is pleaded in the alternative to Plaintiffs' unjust enrichment claim below.

262. Plaintiffs and Class Members were required to provide their Personal Information to Defendant as a condition of receiving medical services and/or employment from Defendant.

263. Plaintiffs and the Class entrusted their Personal Information, directly or indirectly, to Defendant. In so doing, Plaintiffs and the Class entered into implied contracts with Defendant by which Defendant agreed to safeguard and protect such information, to keep such information secure and confidential, and to timely and accurately notify Plaintiffs and the Class if their data had been breached and compromised or stolen.

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

265. Implicit in the agreement between Plaintiffs and Class Members and the Defendant

to provide Personal Information, was the latter's obligation to: (a) use such Personal Information for business purposes only, (b) take reasonable steps to safeguard that Personal Information, (c) prevent unauthorized disclosures of the Personal Information, (d) provide Plaintiffs and Class Members with prompt and sufficient notice of any and all unauthorized access and/or theft of their Personal Information, (e) reasonably safeguard and protect the Personal Information of Plaintiffs and Class Members from unauthorized disclosure or uses, and (f) retain the Personal Information only under conditions that kept such information secure and confidential.

266. The mutual understanding and intent of Plaintiffs and Class Members on the one hand, and Defendant, on the other, is demonstrated by their conduct and course of dealing.

267. Defendant solicited, offered, and invited Plaintiffs and Class Members to provide their Personal Information as part of Defendant's regular business practices. Plaintiffs and Class Members accepted Defendant's offers and provided their Personal Information to Defendant.

268. In accepting the Personal Information of Plaintiffs and Class Members, Defendant understood and agreed that it was required to reasonably safeguard the Personal Information from unauthorized access or disclosure.

269. On information and belief, at all relevant times Defendant promulgated, adopted, and implemented written privacy policies whereby it expressly promised Plaintiffs and Class Members that it would only disclose Personal Information under certain circumstances, none of which relate to the Data Breach.

270. On information and belief, Defendant further promised to comply with industry standards and to make sure that Plaintiffs' and Class Members' Personal Information would remain protected.

271. Plaintiffs and Class Members paid money to Defendant with the reasonable belief

and expectation that Defendant would use part of its earnings to obtain adequate data security. Defendant failed to do so.

272. Plaintiffs and Class Members would not have entrusted their Personal Information to Defendant in the absence of the implied contract between them and Defendant to keep their information reasonably secure.

273. Plaintiffs and Class Members fully and adequately performed their obligations under the implied contracts with Defendant.

274. Defendant breached the implied contracts it made with Plaintiffs and the Class by failing to safeguard and protect their personal information, by failing to delete the information of Plaintiffs and the Class once the relationship ended, and by failing to provide accurate notice to them that personal information was compromised as a result of the Data Breach.

275. As a direct and proximate result of Defendant's breach of the implied contracts, Plaintiffs and Class Members sustained injury-in-fact and damages, as alleged herein, including the loss of the benefit of the bargain.

276. Plaintiffs and Class Members are entitled to compensatory, consequential, and nominal damages suffered as a result of the Data Breach.

277. Plaintiffs and Class Members are also entitled to injunctive relief requiring Defendant to, e.g., (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit monitoring to all Class Members.

COUNT III
BREACH OF THIRD-PARTY BENEFICIARY CONTRACT
(On Behalf of Plaintiffs and the Nationwide Class or, in the Alternative, the State Subclasses)

278. Plaintiffs restate and reallege the preceding factual allegations set forth above as if

fully alleged herein.

279. This count is pleaded in the alternative to Plaintiffs' unjust enrichment claim below.

280. Upon information and belief, PharMerica entered into virtually identical contracts with its healthcare partners to provide pharmaceutical services to them, which included guarantees for reasonable data security practices, procedures, and protocols sufficient to safeguard the Personal Information that was to be entrusted to it.

281. Such contracts were made expressly for the benefit of Plaintiffs and the Class, as it was their Personal Information that Defendant agreed to receive and protect through their services. Thus, the benefit of collection and protection of the Personal Information belonging to Plaintiffs and the Class was the direct and primary objective of the contracting parties, and Plaintiffs and Class Members were direct and express beneficiaries of such contracts.

282. Defendant knew that if they were to breach these contracts with their clients, Plaintiffs and the Class would be harmed.

283. Defendant breached their contracts with its clients and, as a result, Plaintiffs and Class Members were affected by this Data Breach when Defendant failed to use reasonable data security and/or business associate monitoring measures that could have prevented the Data Breach.

284. As foreseen, Plaintiffs and the Class were harmed by Defendant's failure to use reasonable data security measures to securely store and protect the files in their care, including but not limited to, the continuous and substantial risk of harm through the loss of their Personal Information.

285. As a direct and proximate result of Defendant's breach, Plaintiffs and Class Members sustained injury-in-fact and damages, as alleged herein.

286. Accordingly, Plaintiff and the Class are entitled to damages in an amount to be

determined at trial, along with costs and attorneys' fees incurred in this action.

COUNT IV
BREACH OF FIDUCIARY DUTY
(On Behalf of Plaintiffs and the Nationwide Class or, in the Alternative, the State Subclasses)

287. Plaintiffs restate and reallege the preceding factual allegations set forth above as if fully alleged herein.

288. In light of the special relationship between PharMerica and Plaintiffs and Class Members, whereby Defendant became guardian of Plaintiffs' and Class Members' Personal Information, Defendant became a fiduciary by its undertaking and guardianship of the Personal Information, to act primarily for Plaintiffs and Class Members, (1) for the safeguarding of Plaintiffs' and Class Members' Personal Information; (2) to timely notify Plaintiffs and Class Members of a Data Breach and disclosure; and (3) to maintain complete and accurate records of what information (and where) Defendant did and does store.

289. Defendant has a fiduciary duty to act for the benefit of Plaintiffs and Class Members upon matters within the scope of PharMerica's relationship with its patients, in particular, to keep secure their Personal Information.

290. Defendant breached its fiduciary duties to Plaintiffs and Class Members by failing to diligently discover, investigate, and give notice of the Data Breach in a reasonable and practicable period of time.

291. Defendant breached its fiduciary duties to Plaintiffs and Class Members by failing to encrypt and otherwise protect the integrity of the systems containing Plaintiffs' and Class Members' Personal Information.

292. Defendant breached its fiduciary duties owed to Plaintiffs and Class Members by failing to timely notify and/or warn Plaintiffs and Class Members of the Data Breach

293. Defendant breached its fiduciary duties to Plaintiffs and Class Members by otherwise failing to safeguard Plaintiffs' and Class Members' Personal Information.

294. As a direct and proximate result of Defendant's breach of its fiduciary duties, Plaintiffs and Class Members have suffered and will continue to suffer injury-in-fact and damages as alleged herein, and/or harm, and other economic and non-economic losses.

COUNT V
INVASION OF PRIVACY
(On Behalf of Plaintiffs and the Nationwide Class or, in the Alternative, the State Subclasses)

295. Plaintiffs restate and reallege the preceding factual allegations set forth above as if fully alleged herein.

296. Plaintiffs and Class Members had a legitimate expectation of privacy regarding their Private Information and were accordingly entitled to the protection of this information against disclosure to unauthorized third parties.

297. Defendant owed a duty to Plaintiffs and Class Members to keep their Private Information confidential.

298. Defendant acted willfully and affirmatively and recklessly disclosed Plaintiffs' and Class Members' Private Information to unauthorized third parties.

299. The unauthorized disclosure and/or acquisition (i.e., theft) by a third party of Plaintiffs' and Class Members' Private Information is highly offensive to a reasonable person.

300. Defendant's reckless and negligent failure to protect Plaintiffs' and Class Members' Private Information constitutes an intentional interference with Plaintiffs' and Class Members' interest in solitude or seclusion, either as to their person or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

301. In failing to protect Plaintiffs' and Class Members' Private Information,

Defendant acted with a knowing state of mind when it permitted the Data Breach because it knew its information security practices were inadequate.

302. Defendant had notice and knew that its inadequate cybersecurity practices would cause injury to Plaintiffs and the Class and failed to properly safeguard Plaintiffs' and Class Members' Private Information despite that knowledge.

303. Defendant knowingly did not notify Plaintiffs and Class Members in a timely fashion about the Data Breach.

304. As a direct and proximate result of Defendant's acts and omissions, Plaintiffs and the Class Members' private and sensitive Private Information was stolen by a third party and is now available for disclosure and redisclosure without authorization, causing Plaintiffs and Class Members to suffer injury-in-fact and damages as alleged in the preceding paragraphs.

305. Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiffs and Class Members since their Private Information is still maintained by Defendant under inadequate cybersecurity system and policies.

306. Plaintiffs and Class Members have no adequate remedy at law for the injuries relating to Defendant's continued possession of their sensitive and confidential records. A judgment for monetary damages will not end Defendant's inability to safeguard Plaintiffs' and Class Members' Private Information.

307. Plaintiffs, on behalf of themselves and Class Members, seek injunctive relief to enjoin Defendant from further intruding into the privacy and confidentiality of Plaintiffs' and Class Members' Private Information.

308. Plaintiff, on behalf of themselves and Class Members, seek compensatory damages for Defendant's invasion of privacy, which includes the value of the privacy interest invaded by

Defendant, the costs of future monitoring of their credit history for identity theft and fraud, plus prejudgment interest, and costs.

COUNT VI
UNJUST ENRICHMENT
(On Behalf of Plaintiffs and the Nationwide Class or, in the Alternative, the State Subclasses)

309. Plaintiffs restate and reallege the preceding factual allegations set forth above as if fully alleged herein.

310. This count is pleaded in the alternative to Plaintiffs' breach of contract claims above.

311. Plaintiffs and Class Members conferred a monetary benefit on Defendant. Specifically, they paid for services from Defendant and/or its agents and in so doing also provided Defendant with their Personal Information. In exchange, Plaintiffs and Class Members should have received from Defendant the services that were the subject of the transaction and should have had their Personal Information protected with adequate data security.

312. Defendant knew that Plaintiffs and Class Members conferred a benefit on it in the form their Personal Information as well as labor in connection with employment, and payments made on their behalf as a necessary part of their receiving healthcare services. Defendant appreciated and accepted that benefit. Defendant profited from these transactions and used the Personal Information of Plaintiffs and Class Members for business purposes.

313. Upon information and belief, Defendant funds its data security measures entirely from its general revenue, including payments on behalf of or for the benefit of Plaintiffs and Class Members.

314. As such, a portion of the payments made for the benefit of or on behalf of Plaintiffs and 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.

315. Defendant, however, failed to secure Plaintiffs' and Class Members' Personal Information and, therefore, did not provide adequate data security in return for the benefit Plaintiffs and Class Members provided. Defendant has been knowingly enriched by diverting funds to its own profit that should have been reasonably expended to protect the personal information of Plaintiffs and the Class

316. Defendant would not be able to carry out an essential function of its regular business without the Personal Information of Plaintiffs and Class Members and derived revenue by using it for business purposes. Plaintiffs and Class Members expected that Defendant or anyone in Defendant's position would use a portion of that revenue to fund adequate data security practices.

317. Defendant acquired the Personal Information through inequitable means in that it failed to disclose PharMerica's inadequate security practices previously alleged.

318. If Plaintiffs and Class Members knew that Defendant had not reasonably secured their Personal Information, they would not have allowed their Personal Information to be provided to Defendant.

319. Defendant enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiffs' and Class Members' Personal Information. Instead of providing a reasonable level of security that would have prevented the hacking incident, Defendant instead calculated to increase its own profit at the expense of Plaintiffs and Class Members by utilizing cheaper, ineffective security measures and diverting those funds to its own profit. Plaintiffs 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 and the safety of

their Personal Information.

320. Under the principles of equity and good conscience, Defendant should not be permitted to retain the money wrongfully obtained Plaintiffs and Class Members, because Defendant failed to implement appropriate data management and security measures that are mandated by industry standards.

321. Plaintiffs and Class Members have no adequate remedy at law.

322. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have suffered and will continue to suffer injury-in-fact and damages and/or harm as alleged in the preceding paragraphs.

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

COUNT VII
VIOLATIONS OF KENTUCKY'S CONSUMER PROTECTION ACT
(Ky. Rev. Stat. Ann. § 367.110, *et seq*.)
(On Behalf of Plaintiffs and the Class)

324. Plaintiffs restate and reallege the preceding factual allegations set forth above as if fully alleged herein.

325. Plaintiffs and Class Members are "persons" as defined by Ky. Rev. Stat. Ann. § 367.110.

326. The acts and practices described herein are within the scope of "trade" and "commerce" as defined by Ky. Rev. Stat. Ann. § 367.110.

327. In connection with its consumer transactions, Defendant engaged in unfair or unconscionable practices and acts by, *inter alia*, failing to comply with applicable state and federal

laws and industry standards pertaining to data security, including the FTC Act and HIPAA, soliciting and collecting Plaintiffs' and Class Members' Personal Information with knowledge that the information would not be adequately protected, storing Plaintiffs' and Class Members' Personal Information in an unsecure electronic environment, and failing to take proper action following the Data Breach to enact adequate privacy and security measures and protect Plaintiffs' and Class Members' Personal Information and other personal information from further unauthorized disclosure, release, and data breaches.

328. Defendant's unfair, deceptive, and unconscionable practices and acts were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to Plaintiffs and Class Members that they could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

329. Defendant acted intentionally, knowingly, and maliciously in violating the Act, and recklessly disregarded Plaintiffs and Class Members' rights. Only Defendant was aware of the security deficiencies in its data systems. Consumers, including Plaintiffs and Class Members, lacked this knowledge and consumers lack expertise in information security. Even if they did have this expertise, consumers do not have access to Defendant's data systems to ensure the security of their Personal Information.

330. As a direct and proximate result of Defendant's unfair, deceptive, and unconscionable trade practices, Plaintiffs and Class Members have suffered and will continue to suffer injury, ascertainable losses of money or property, including the diminution in value of their Personal Information, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Personal Information.

331. Plaintiffs and Class Members seek all monetary and nonmonetary relief allowed by law, including actual damages, punitive damages, and equitable relief under Ky. Rev. Stat. Ann. § 367.220 and reasonable attorneys' fees and costs.

COUNT VIII
VIOLATIONS OF MICHIGAN'S DATA BREACH PROMPT NOTIFICATION LAW (MICH. COMP. LAWS ANN. § 445.72(1), *et seq.*)
(On Behalf of Plaintiff Young and the Michigan Class)

332. Plaintiff Young re-alleges and incorporates by reference all other paragraphs in the Complaint as if fully set forth herein.

333. Defendant is required to accurately and timely notify Plaintiff Young and Michigan Subclass members if it discovers a security breach or receives notice of a security breach (where unencrypted and unredacted Personal Information was accessed or acquired by unauthorized persons), without unreasonable delay under Mich. Comp. Laws Ann. § 445.72(1).

334. PharMerica is a business that owns or licenses computerized data that includes personal information as defined by Mich. Comp. Laws Ann. § 445.72(1).

335. Plaintiffs and Class Members' personal information (e.g., Social Security numbers) includes personal information as covered under Mich. Comp. Laws Ann. § 445.72(1).

336. Because PharMerica discovered a security breach and had notice of a security breach (where unencrypted and unredacted personal information was accessed or acquired by unauthorized persons), PharMerica had an obligation to disclose such in a timely and accurate fashion as mandated by Mich. Comp. Laws Ann. § 445.72(4).

337. PharMerica has stated that the Data Breach occurred on March 14, 2023 and Pharmerica was also aware that Money Message began publicly posting the Personal Information stolen in the Data Breach in early April. However, PharMerica did not notify Plaintiff Young and the Michigan Class until approximately June 14, 2023, three months after it discovered the Data

Breach and more than two months after it confirmed that Personal Information had been publicly disclosed.

338. As a direct and proximate result of PharMerica's violations of Mich. Comp. Laws Ann. § 445.72(4), Plaintiff Young and Michigan Class Members suffered injury-in-fact and damages as set forth herein.

339. Plaintiff Young and Michigan Class Members seek all relief available under Mich. Comp. Laws Ann. § 445.72(15), and any other relief the Court deems proper.

COUNT IX
Violation of California's Unfair Competition Law ("UCL")
Unlawful Business Practice
(Cal Bus. & Prof. Code § 17200, *et seq*.)
(On Behalf of Plaintiffs Molina, Luther and the California Subclass)

340. Plaintiffs Molina and Luther re-allege and incorporate by reference all other paragraphs in the Complaint as if fully set forth herein.

341. Defendant engaged in unlawful and unfair business practices in violation of Cal. Bus. & Prof. Code § 17200, *et seq*. which prohibits unlawful, unfair, or fraudulent business acts or practices ("UCL").

342. Defendant's conduct is unlawful because it violates the California Consumer Privacy Act of 2018, Civ. Code § 1798.100, et seq. (the "CCPA"), and other state data security laws.

343. Defendant stored the Personal Information of Plaintiffs and the California Subclass in its computer systems and knew or should have known it did not employ reasonable, industry standard, and appropriate security measures that complied with applicable regulations and that would have kept Plaintiffs' and the California Subclass's Personal Information secure so as to prevent the loss or misuse of that Personal Information.

344. Defendant failed to disclose to Plaintiffs and the California Subclass that their

Personal Information was not secure. However, Plaintiffs and the California Subclass were entitled to assume, and did assume, that Defendant had secured their Personal Information. At no time were Plaintiffs and the California Subclass on notice that their Personal Information was not secure, which Defendant had a duty to disclose.

345. Defendant also violated California Civil Code § 1798.150 by failing to implement and maintain reasonable security procedures and practices, resulting in an unauthorized access and exfiltration, theft, or disclosure of Plaintiffs' and the California Subclass's nonencrypted and nonredacted PII.

346. Had Defendant complied with these requirements, Plaintiffs and the California Subclass would not have suffered the damages related to the data breach.

347. Defendant's conduct was unlawful, in that it violated the CCPA.

348. Defendant's acts, omissions, and misrepresentations as alleged herein were unlawful and in violation of, inter alia, Section 5(a) of the Federal Trade Commission Act.

349. Defendant's conduct was also unfair, in that it violated a clear legislative policy in favor of protecting consumers from data breaches.

350. Defendant's conduct is an unfair business practice under the UCL because it was immoral, unethical, oppressive, and unscrupulous and caused substantial harm. This conduct includes employing unreasonable and inadequate data security despite its business model of actively collecting Personal Information.

351. Defendant also engaged in unfair business practices under the "tethering test." Its actions and omissions, as described above, violated fundamental public policies expressed by the California Legislature. See, e.g., Cal. Civ. Code § 1798.1 ("The Legislature declares that . . . all individuals have a right of privacy in information pertaining to them . . . The increasing use of

computers . . . has greatly magnified the potential risk to individual privacy that can occur from the maintenance of personal information."); Cal. Civ. Code § 1798.81.5(a) ("It is the intent of the Legislature to ensure that personal information about California residents is protected."); Cal. Bus. & Prof. Code § 22578 ("It is the intent of the Legislature that this chapter [including the Online Privacy Protection Act] is a matter of statewide concern."). Defendant's acts and omissions thus amount to a violation of the law.

352. Instead, Defendant made the Personal Information of Plaintiffs and the California Subclass accessible to scammers, identity thieves, and other malicious actors, subjecting Plaintiffs and the California Subclass to an impending risk of identity theft. Additionally, Defendant's conduct was unfair under the UCL because it violated the policies underlying the laws set out in the prior paragraph.

353. As a result of those unlawful and unfair business practices, Plaintiffs and the California Subclass suffered an injury-in-fact and damages as set forth herein, and have lost money or property as they would not have entered into transactions with Defendant or would not have provided their personal information to Defendant had Defendant disclosed its substandard data security practices.

354. The injuries to Plaintiffs and the California Subclass greatly outweigh any alleged countervailing benefit to consumers or competition under all of the circumstances.

355. There were reasonably available alternatives to further Defendant's legitimate business interests, other than the misconduct alleged in this complaint.

356. Therefore, Plaintiffs and the California Subclass are entitled to equitable relief, including restitution of all monies paid to or received by Defendant; disgorgement of all profits accruing to Defendant because of its unfair and improper business practices; a permanent

injunction enjoining Defendant's unlawful and unfair business activities; and any other equitable relief the Court deems proper.

COUNT X
Violation of the California Consumer Records Act
Cal. Civ. Code § 1798.80, *et seq*.
(On Behalf of Plaintiff Molina, Luther and the California Subclass)

357. Plaintiffs Molina and Luther re-allege and incorporate by reference all other paragraphs in the Complaint as if fully set forth herein.

358. Under California law, any "person or business that conducts business in California, and that owns or licenses computerized data that includes personal information" must "disclose any breach of the system following discovery or notification of the breach in the security of the data to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person." (Cal. Civ. Code § 1798.82.) The disclosure must "be made in the most expedient time possible and without unreasonable delay" (Id.), but "immediately following discovery [of the breach], if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person." (Cal. Civ. Code § 1798.82, subdiv. b.)

359. The Data Breach constitutes a "breach of the security system" of Defendant.

360. An unauthorized person acquired the personal, unencrypted information of Plaintiffs and the California Subclass.

361. Defendant knew that an unauthorized person had acquired the personal, unencrypted information of Plaintiffs and the California Subclass, but waited three months to notify them. Three months was an unreasonable delay under the circumstances.

362. Defendant's unreasonable delay prevented Plaintiffs and the California Subclass from taking appropriate measures from protecting themselves against harm.

363. Because Plaintiffs and the California Subclass were unable to protect themselves, they suffered incrementally increased damages that they would not have suffered with timelier notice.

364. Plaintiffs and the California Subclass are entitled to equitable relief and damages in an amount to be determined at trial.

COUNT XI
Violation of the California Consumer Privacy Act
Cal. Civ. Code § 1798.150
(On Behalf of Plaintiff Molina, Luther and the California Subclass)

365. Plaintiffs Molina and Luther re-allege and incorporate by reference all other paragraphs in the Complaint as if fully set forth herein.

366. Defendant violated California Civil Code § 1798.150 of the CCPA by failing to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the nonencrypted Personal Information of Plaintiff and the California Subclass. As a direct and proximate result, Plaintiffs', and the California Subclass's nonencrypted and nonredacted Personal Information was subject to unauthorized access and exfiltration, theft, or disclosure.

367. Defendant is a business organized for the profit and financial benefit of its owners according to California Civil Code § 1798.140, that collects the personal information of its customers and employees, and whose annual gross revenues exceed the threshold established by California Civil Code § 1798.140(d).

368. Plaintiffs and California Subclass Members seek injunctive or other equitable relief to ensure Defendant hereinafter adequately safeguards Personal Information by implementing reasonable security procedures and practices. Such relief is particularly important because Defendant continues to hold PII, including Plaintiffs' and California Subclass members' Personal

Information. Plaintiffs and California Subclass members have an interest in ensuring that their Personal Information is reasonably protected, and Defendant has demonstrated a pattern of failing to adequately safeguard this information.

369. Pursuant to California Civil Code § 1798.150(b), on July 19, 2023, Plaintiffs mailed a CCPA notice letter to Defendant's registered service agents, detailing the specific provisions of the CCPA that Defendant has violated and continues to violate.

370. On August 18, 2023, Defendant responded to Plaintiffs' CCPA notice letter claiming "that any alleged CCPA violations related to the Data Incident have been cured and no further violations shall occur." However, Defendant provided neither evidence nor assurances that the information compromised in the Data Breach had been successfully retrieved or destroyed to ensure that no risk of identity theft or fraud remains as a result of the Data Breach.

371. Accordingly, because no cure is possible under these facts and circumstances—Plaintiffs intend to seek statutory damages of between $100 and $750, in addition to all other relief afforded by the CCPA.

COUNT XII
Violation of the California Confidentiality of Medical Information Act ("CMIA"), Cal. Civ. Code § 56, *et seq.*
(On Behalf of Plaintiffs Molina, Luther and the California Subclass)

372. Plaintiffs Molina and Luther re-allege and incorporate by reference all other paragraphs in the Complaint as if fully set forth herein.

373. Section 56.10(a) of the California Civil Code provides that "[a] provider of health care, health care service plan, or contractor shall not disclose medical information regarding a patient of the provider of health care or an enrollee or subscriber of a health care service plan without first obtaining an authorization[.]"

374. Defendant is a "healthcare provider" within the meaning of Civil Code § 56.05 and

Civil Code § 56.06 and/or a "business organized for the purpose of maintaining medical information" and/or a "business that offers software or hardware to consumers . . . that is designed to maintain medical information" within the meaning of Civil Code § 56.06(a) and (b), and maintained and continues to maintain "medical information," within the meaning of Civil Code § 56.05(j), for "patients" of Defendant, within the meaning of Civil Code § 56.05(k).

375. Plaintiffs and California subclass members are "patients" within the meaning of Civil Code § 56.05(k) and are "endanger[ed]" within the meaning of Civil Code § 56.05(e) because Plaintiffs and California subclass members fear that disclosure of their medical information could subject them to harassment or abuse.

376. Plaintiffs and California subclass members, as patients, had their individually identifiable "medical information," within the meaning of Civil Code § 56.05(j), created, maintained, preserved, and stored on Defendant's computer network at the time of the unauthorized disclosure.

377. Defendant, through inadequate security, allowed unauthorized third-party access to Plaintiffs' and California subclass members' medical information, without the prior written authorization of Plaintiffs and California subclass members, as required by Civil Code § 56.10 of the CMIA.

378. In violation of Civil Code § 56.10(a), Defendant disclosed Plaintiffs' and California subclass members' medical information without first obtaining an authorization. Plaintiffs' and California subclass members' medical information was viewed by unauthorized individuals as a direct and proximate result of Defendant's violation of Civil Code § 56.10(a).

379. In violation of Civil Code § 56.10(e), Defendant further disclosed Plaintiffs' and California subclass members' medical information to persons or entities not engaged in providing

direct health care services to Plaintiffs or California subclass members, or to their providers of health care or health care service plans or their insurers or self-insured employers.

380. Defendant violated Civil Code § 56.101 of the CMIA through its willful and knowing failure to maintain and preserve the confidentiality of the medical information of Plaintiffs and the California subclass members. Defendant's conduct with respect to the disclosure of confidential PII and PHI was willful and knowing because Defendant designed and implemented the computer network and security practices that gave rise to the unlawful disclosure.

381. In violation of Civil Code § 56.101(a), Defendant created, maintained, preserved, stored, abandoned, destroyed, or disposed of Plaintiffs' and class members' medical information in a manner that failed to preserve and breached the confidentiality of the information contained therein. Plaintiffs' and California subclass member' medical information was viewed by unauthorized individuals as a direct and proximate result of Defendant's violation of Civil Code § 56.101(a). 380. In violation of Civil Code § 56.101(a), Defendant negligently created, maintained, preserved, stored, abandoned, destroyed, or disposed of Plaintiffs' and California subclass members' medical information. Plaintiffs' and California subclass members' medical information was viewed by unauthorized individuals as a direct and proximate result of Defendant's violation of Civil Code § 56.101(a).

382. Plaintiffs' and California subclass members' medical information that was the subject of the unauthorized disclosure included "electronic medical records" or "electronic health records" as referenced by Civil Code § 56.101(c) and defined by 42 U.S.C. § 17921(5).

383. In violation of Civil Code § 56.101(b)(1)(A), Defendant's electronic health record system or electronic medical record system failed to protect and preserve the integrity of electronic medical information. Plaintiffs' and California subclass members' medical information was

viewed by unauthorized individuals as a direct and proximate result of Defendant's violation of Civil Code § 56.101(b)(1)(A).

384. Defendant violated Civil Code § 56.36 of the CMIA through its failure to maintain and preserve the confidentiality of the medical information of Plaintiffs and the California subclass members.

385. As a result of Defendant's above-described conduct, Plaintiffs and California subclass members have suffered damages from the unauthorized disclosure and release of their individual identifiable "medical information" made unlawful by Civil Code §§ 56.10, 56.101, 56.36. 385.

386. As a direct and proximate result of Defendant's above-described wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused the unauthorized disclosure, and violation of the CMIA, Plaintiffs and California subclass members have suffered (and will continue to suffer) economic damages and other injury and actual harm in the form of, inter alia, (i) an imminent, immediate and the continuing increased risk of identity theft, identity fraud and medical fraud-risks justifying expenditures for protective and remedial services for which they are entitled to compensation, (ii) invasion of privacy, (iii) breach of the confidentiality of their PII and PHI, (iv) statutory damages under the California CMIA, (v) deprivation of the value of their PII and PHI, for which there is a well-established national and international market, and/or (vi) the financial and temporal cost of monitoring their credit, monitoring their financial accounts, and mitigating their damages.

387. Plaintiffs, individually and for each member of the California Subclass, seek nominal damages of one thousand dollars ($1,000) for each violation under Civil Code § 56.36(b)(1), and actual damages suffered, if any, pursuant to Civil Code § 56.36(b)(2),

injunctive relief, as well as punitive damages of up to $3,000 per Plaintiff and each California subclass member, and attorneys' fees, litigation expenses and court costs, pursuant to Civil Code § 56.35.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, David Hibbard, Frank Raney, James Young, Holly Williams, Micaela Molina, and Charley Luther, individually, and on behalf of all others similarly situated, pray for judgment as follows:

A. For an Order certifying this action as a class action and appointing Plaintiffs and their counsel to represent the Class and Subclasses;

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

C. For equitable relief compelling Defendant to utilize appropriate methods and policies with respect to consumer data collection, storage, and safety, and to disclose with specificity the type of Personal Information compromised during the Data Breach;

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

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

ii. Requiring Defendant to protect, including through encryption, all data collected through the course of its business in accordance with all

applicable regulations, industry standards, and federal, state, or local laws;

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

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

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

vi. Requiring Defendant to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

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

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

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

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

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

xii. Requiring Defendant to routinely and continually conduct internal training and education, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

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

xiv. Requiring Defendant to implement, maintain, regularly review, and revise as necessary a threat management program designed to

appropriately monitor Defendant's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

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

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

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

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

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

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

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

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

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

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

JURY TRIAL DEMANDED

Plaintiffs demand a trial by jury on all claims so triable.

Dated: January 12, 2024

Respectfully submitted,

s/ J. Gerard Stranch, IV

J. Gerard Stranch, IV (Admitted *Pro Hac Vice*)
STRANCH, JENNINGS & GARVEY, PLLC
The Freedom Center
223 Rosa L. Parks Avenue, Suite 200
Nashville, Tennessee 37203
Tel.: 615-254-8801
Fax: 615-255-5419
gstranch@stranchlaw.com

Interim Lead Counsel

E. Michelle Drake (Admitted *Pro Hac Vice*)
BERGER MONTAGUE, PC
43 SE Main Street, Suite 505
Minneapolis, Minnesota 55414
Tel.: 612-594-5999
Fax: 612-584-4470
emdrake@bm.net

Gary Klinger (Admitted *Pro Hac Vice*)
MILBERG COLEMAN PHILLIPS GROSSMAN, PLLC
227 W. Monroe Street, Suite 2100
Chicago, Illinois 60606
Tel.: (866) 252-0878
gklinger@milberg.com

Lynn A. Toops (Admitted *Pro Hac Vice*)
COHEN & MALAD, LLP
One Indiana Square, Suite 1400

Indianapolis, Indiana 46204
Tel: (317) 636-6481
Fax: (317) 636-2539
ltoops@cohenandmalad.com

Co-Members of Plaintiffs' Executive Committee

Augustus Herbert
GRAY ICE HIGDON, PLLC
3939 Shelbyville Road, Suite 201
Louisville, Kentucky 40207
Direct: 502.625.2732
Fax: 502.561.0442
aherbert@grayice.com

Liaison Counsel

ATTORNEYS FOR PLAINTIFFS

CERTIFICATE OF SERVICE

It is hereby certified that a true and accurate copy of the foregoing was this 12th day of January 2024 filed via the CM/ECF system, which will electronically serve all counsel of record.

s/ J. Gerard Stranch, IV
J. Gerard Stranch, IV

Interim Lead Counsel

EXHIBIT A

GO BACK TO THE MAIN PAGE

Money Message

Hello!

< 1 ... 9 10 11 12 13 ... 17 >

Pharmerica.com & BrightSpring Health Services

28.03.2023

Headquartered in Louisville, Kentucky, PharMerica is one of the largest and fastest-growing institutional pharmacy companies in the United States. Our premier pharmacy services, with more than 180 long-term care pharmacies in almost every state, have a national scope but a local approach. Revenue: $3B

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. We focus on providing quality outcomes, through best-in-class service and technology capabilities. Revenue: $5.4B

We have 2 millions records of that type and we'll publish them if they don't want to pay. Each time we'll publish more and more records at once.

UPD3: we add 500 more records and few tables from the DB. Enjoy!

UPDATE4: link to files

UPDATE5: 4.7TB DB with 1.6M minimum records of personal data including ESN & DOB. Link will be revealed soon

Download Granted to be top 100.xlsx
Download 2nd_portion.zip
Download Update_3.zip

http://au6l74lej2qvwrvasdyc5ta4g7jdshjwkzbi635g6uztld2n2fcacyad.onion

EXHIBIT B

InsPlanOptionValues
PatientE1TransactionHistoryLog
PatientMOPs
RxBatches
Errors
HL7RouteTranslationsLog
EquivalentProducts
ArchiveErrorLog
DistributionCds
DeliveryRoutes
InsPlanPartDPlansLog
RxChangeRequestRxECSFields
UPSPackTypes
DeliveryAgentsLog
InsPlanPartDPlans
PatientMopSpecProdCovers
MegaRuleDrugsLog
StatementFormatsLog
RxChecklistItems
ERxAuditLog
vVaccinationProviders
CustomFieldDefsLog
eRxQueueFolderRuleFacilities
PharmacyRxChecklistItemsLog
RestoreQueue
Items
RxChangeRequestRxIngreds
UPSServices
FacilityRoomsLog
ReorderClarificationCdsLog
InsPlanPharmECS
NursingStationCustomFields
PatientNoteHistory
DeliveryRoutesLog
PostItTypesLog
RxChecklistItemsLog
ExternalInterfaceIDs
SplitHRxsLog
PhTheraChangeLevelContacts
eRxQueueFolderRuleMsgTypes
PersonCentricAdminTimeTranslationsLog
QBAccounts
UPSWorldShipInterface
InventoryTaxStatusLog
TargetPopulations
FacAdminTimesLog
InsPlans
PatientLitOrdAdminTimesLog
NursingStationCustomFieldsLog
PatientNotes

RestoreLog
RxClarificationCds
FlowFormats
IncomingHL7MessagesLog
eRxQueueFolderRulePharmacies
MegaRuleDrugs
QBCustomers
PendingOrdersERx
InsPlanPharmECSLog
UserDrugs
DischargeReasonsLog
InsPlansAuditLog
PatientPackageTypes
RestoreErrorLog
SubMenuIdsLog
RxClinicalWarnings
FwHL7Interfaces
CustomReportFoldersLog
eRxQueueFolderRules
submenuids_backup_20220708
PharmacyTeamsLog
EdpUserFacilities
QBItems
EdpUserNursingStations
WebUserAccess
FacilityTaxStatusLog
InventoryCountSessions
ReorderCompositeFillNumbersLog
InsPlansAuditLogFields
PatientPerDiemEligibility
ArchiveSourceQueryOverride
DeliveryAgentDayRouteOverrides
PrnDefsLog
RxCustomFields
FwInterfaces
ToteAssignsLog
NursingStationOptionCategoriesLog
eRxQueueFolders
PhTheraChangeLog
QBTerms
UserNursingStationChanges
WebUsers
InventoryZonesLog
FacBlockedWLblCdsLog
InsPlanSharedCopay
PatientLitOrdsLog
Patients
UserFacilityChanges
DeliveryAgentDayRoutes
RxDirections

InventoryCounts
GeriMedFiles
InstallationsLog
eRxQueueFolderUsers
PackingSlipArchiveLabelDetail
TaxGroups
InsPlansLog
DrugCategoriesLog
ApiMethods
InsPlansPBMCoverage
PatientsInterfaced
SystemOptionCategoriesLog
RxECSFields
HL7AllergyTranslations
CustomReportsLog
ExternalMedIds
PharmacyUserCostsLog
ApiLog
FacPackageTypesLog
ReorderCustomFieldsLog
InsPlanWrngs
PatientsLog
PackingSlipArchivePatientDetail
DeliveryRouteLocationStatus
PrnNamesLog
RxIngreds
HL7Messages
ToteAssignsHistoryLog
FeeSched
PhysicianCustomFieldsLog
UserFacilityAdminData
MTMEligImportsLog
FacContactsLog
InvoiceGrps
PatientLitOrdsInterfacedLog
PatientTaxStatus
ECMAssociationModificationQueue
DeliveryRouteReturns
RxLabels
HL7PendingTQD
InterchangeIDQualifiersLog
HPODetail
PackingSlipArchiveRxDetail
InsPlanSharedCopayLog
vRxDirections
DrugCategoryDefsLog
DeliveriesSort
LitCatCds
PatientViews
DrugDisposalLog

SystemOptionsLog
DeliveryRouteRxStatus
vRxAdminTimes
RxPickups
HL7RouteNames
CustomReportSecurityLog
HPOHeaders
PharmRxNumbersLog
FacPackagingGroupExceptionsLog
DeliveryRoutesSort
ReorderDirectionsLog
LitIdAdminTimes
PatientXfers
DrugDisposalLogExternalMetadata
PrnTypesLog
Rxs
HL7RouteTranslations
WorkflowOverridesLog
Inventory
PhysicianFacilitiesLog
DeliveryRouteStatus
NDCStatusCodesLog
FacCustomerNosLog
LitIDs
PatientMCareCyclesLog
PatPackagingGroupExceptions
RxAuthReqd
RxsInterfaced
IncomingHL7Messages
PendingReturnItems
InventoryAdjustmentCodesLog
InventoryActPkgCostHist
LOALog
ApiCallLog
InsPlansPBMCoverageLog
DrugZonesLog
MARGroups
PatPackagingGroups
AdminScheds
TSFormatsLog
RxDashboard
SplitHRxs
ProductUserSessions
Installations
DeliveredTotePackingSlipID
VaccinationNDCMap
DischargeFormatsLog
InventoryAuditLog
PODetailLog
FacRoNumbersLog

PendingReturnItemsOtherPharmacy
ReorderDocsLog
MARMessages
ReorderAuthorizations
FormatDefinitions
CareLvlCds
DeliveryRouteStopStatus
ProcedureModifierCodesLog
ToteAssigns
InstallShield
UserFavoriteRibbons
InventoryAuditLogFields
PhysiciansLog
OnSiteStoreInventoryLog
ProductUserSessionTokens
InterchangeIDQualifiers
VaccinationAPIRequests
FacDeliverySchedLog
NsDeliverySched
PatientMopActiveDatesLog
ReorderAuthorizationsAuditLog
CareLvlLocations
ToteAssignsHistory
NDCChangesHistory
Returns
InvoiceNumbersLog
InventoryAvgUnitCostHist
PackListCommentsLog
InsPlanWrngsLog
InterfaceQueue
eCourierSettingsLog
StructuredSigCodeTimingTypes
CustomerGroupsLog
NsDoNotSendItems
ReorderClarificationCds
DefaultMarGroups
UPSBillOptsLog
WorkflowOverrides
DiscontinuedMedNoticesLog
InventoryCustomFields
NsHouseStockLog
POHeadersLog
vReleasedRxs
FacTypeDefsLog
InterfaceQueueErrors
ReorderIngredsLog
NursingStationAdminTimes
ReorderCompositeFillNumbers
DefInvoiceGrps
DeliveryRouteToteStatus

ProgIDsLog
vReleasedPsIDs
ReturnItems
InventoryLog
PhysicianTypesLog
OnSiteStoresLog
ReorderRecertifications
InterfaceQueueLog
SystemAttributes
FacDoNotSendItemsLog
NursingStationCycles
PatientMopAdditionalInfoLog
ReorderCustomFields
Deliveries
ReturnItemsOtherPharmacy
LabelFormatsLog
InventoryPartialReturnValidations
PARHistoryLog
InvoiceGrpsLog
vExpirationDateByCcidOrGpi
InventoryAdjustmentCodes
EquivalentProductsLog
CustomersLog
NursingStationGroups
NsHouseStock
ReorderDirections
XMLQueueAssigns
DrugAuthorizations
UPSPackTypesLog
RouteStops
vExpDateByCcidOrGpiAudit
DrugQuoteNDCStatusCodes
DSFormatsLog
InventoryReturns
PricingLog
GlobalLitOrdAdminTimesLog
InvoiceNumbers
ReorderRequestsLog
ReportBillingSummaryByMethodOfPaymentResults
NursingStationPackageTypes
ReorderDocs
ExternalFacilityIDs
PSFormatsLog
InventoryTaxStatus
NsFormularyLog
PlanBenefitManagersLog
XMLQueueCategory
OnSiteStoreTemplateInventoryLog
RxRequests
LabelFormats

FacFormularyLog
NursingStations
PatientMopEcsFieldsLog
ReorderIngreds
ExternalNursingStationIDs
StopLocations
LockProcessesLog
InventoryZones
PaymentsLog
LitCatCdsLog
HRxRequests
LockProcesses
eRxQueueFolderRuleFacilitiesLog
DistributionCdsLog
PackagingGroups
ReorderRequests
FacAdminTimes
UPSServicesLog
RevertClaimLog
DURRulesLog
MTMEligDetail
ReconstitutionConcentrationsLog
XMLQueueDetails
submenuids_backup_20220712
GlobalLitOrdsLog
TreatmentTypes
MARFormats
ReordersLog
PatientStatusNames
NsFormulary
Reorders
FacBlockedWLblCds
AvailableDeliveriesDriver
QualityEventReasonDefsLog
MTMEligImports
StandingLitOrdAdminTimesLog
OnSiteStoreTemplatesLog
MDLFormats
InsPlanSCCDefaults
FacFwHL7InterfacesLog
Counties
PerDiemFormulary
PatientMopPriceMatchLog
ReordersAdminTimes
FacContacts
CSExportConfig
MARFormatsLog
NDCStatusCodes
PrescriptionsLog
DeliveryAgentDevices

LitIdAdminTimesLog
PharmacyPdmpSetup
MenuIds
eRxQueueFolderRuleMsgTypesLog
InsPlanSCCDefaultsLog
ItemsLog
PerDiemRates
ReordersECSCds
FacCustomerNos
UPSWorldShipInterfaceLog
StructuredSigDeliveryMethods
ECMAssociationTypeLog
OnSiteStoreInventory
ReconstitutionDefinitionsLog
WorkQueue
GlobalLitOrdsInterfacedLog
MinQtys
ReordersAdminTimesLog
GuardianTypes
PersonCentricAdminTimeTranslations
ReorderSingleAuthorizations
FacDeliverySched
QualityEventReasonsLog
StructuredSigDoseForms
OnSiteStoreLog
StandingLitOrdsLog
CSExportPharmacies
DeliveryAgentLocationHistories
OSSPackingSlipHistoryLog
OAFormats
FacGroupDefsLog
PhTheraChange
PatientMopPriceOverridesLog
ReordersInterfaced
WorkQueueComment
FacDoNotSendItems
CSExportConfigLog
StructuredSigRoutes
MDLFormatsLog
OnSiteStores
RefillRemindersLog
DeliveryAgentLocations
LitIDsLog
CustomReportsDisplayLog
PdmpQueryByGPI
OpenRxBatches
eRxQueueFolderRulePharmaciesLog
QBAccountsLog
PhTheraChangeLog
WorkQueueStatus

FacFormulary
UserDrugsLog
StructuredSigTimingCodes
OnSiteStoreTemplateInventory
RemindersLog
PdmpQueryByCCID
HFacAdminTimesLog
ORFormats
ReordersECSCdsLog
PhysicianCustomFields
WorkQueueStatusActivity
FacFwHL7Interfaces
DispatchMessages
QualityEventsLog
OnSiteStoreTemplates
ActivityLogLog
OssQtyConversionsLog
eRxTriageFolderColorRules
PdmpQueryByGPI
PassportTransactionIDs
FacGroupsLog
PhysicianFacilities
PatientMOPsLog
FacGroupDefs
ProductLicenseUpdate
MenuIdsLog
OSSPackingSlipHistory
RTSWarningsLog
CSExportPharmaciesLog
PushNotifications
MARGroupsLog
eRxTriageFolderColorRulesLog
PdmpQueryByCCID
DeliveryRouteStatusLog
PatientNoteDescriptions
eRxQueueFolderRulesLog
ReportFinancialImpactRegistry
QBCustomersLog
Physicians
vClaimsStatus
FacGroups
AutoPatientIdsLog
ECSFieldsLog
OssQtyConversions
RxStatIDsLog
vPdmpQueryByCcidOrGpi
HNursingStationAdminTimesLog
PhProgFormats
ReportFinancialImpactResults
ReorderSingleAuthorizationsLog

PhysiciansAuditLog
FacHouseStock
RxScans
vPdmpQueryByCcidOrGpiAudit
QualityEventTypesLog
PackageTypes
ADLFormatsLog
PackageTypesLog
PkgLblFormats
ReportBillingSummaryByMethodOfPaymentRegistry
FacHouseStockLog
PhysiciansAuditLogFields
PatientMopSpecProdCoversLog
Facilities
MinQtysLog
PackingSlipIDs
MARMessagesLog
rxs_backup_20220617
POFFormats
eRxQueueFoldersLog
QBItemsLog
PhysicianTypes
FacilitiesAuditLog
ExternalPatientIDsLog
ToteAssignScans
ECSFieldValuesLog
PackSlipPrintLog
TaxAuthoritiesLog
ApiTrackingLog
InsFormularyIDsLog
PostIt
ReordersInterfacedLog
PlanBenefitManagers
FacilitiesAuditLogFields
QualityEventUsersLog
PackTypeDailyFees
VaccAdminRoute
APFFormatsLog
ApiTrackingSpecificLog
PackingSlipIDsLog
PostItActions
FacilitiesLog
StandingLitOrdAdminTimes
PatientNoteHistoryLog
FacilityAdmissionForms
OAFormatsLog
Pharmacies
VaccAdminSite
vReleasableRxLabels
NsDeliverySchedLog

PostItCatCds
eRxQueueFolderUsersLog
QBTermsLog
StandingLitOrds
NursingStationOptions
FacilityBeds
FamCustomerNosLog
FileParsingSpecifications
ECSRejectCdsLog
PharmacistFLQueueFacilities
VFCEligibility
UserAltPharmaciesLog
InsGroupsLog
PostItTypes
AddlNDCVendorsLog
NursingStationOptionsLog
FacilityCustomFields
RawBCsLog
Pharmacists
VaccCompletionStatus
ASAP2007IDQualifiersLog
vOrderStatus
PackTypeDailyFeesLog
Agents
PrnDefs
FacilityAdmissionFormsLog
PatientNotesLog
FacilityDocs
OpenRxBatchesLog
PharmacistTeams
NsDoNotSendItemsLog
PrnNames
ExternalMedIdsLog
TaxGroupsLog
FacilityLinkAlerts
FamIDsLog
AgentTables
ActivityLog
ExternalInterfaceIDsLog
PharmacyCustomFields
VaccinationBatches
NursingStationOptionCategories
VendorsLog
InsPlanCustomerNosLog
PrnTypes
AllowablePharmaciesLog
FacilityNotes
DbRevLog
ReturnAdjustmentReasonsLog
ADLFormats

PharmacyLicenses
Vaccinations
NursingStationOptionValues
ASAP2007JurisdictionsLog
PharmaciesLog
FwHL7QMgrConfig
ProcedureModifierCodes
Languages
FacilityBedsLog
PatientPackageTypesLog
FacilityOptionCategories
ORFormatsLog
DeliverySigneeTitles
APFFormats
PharmacyOptionCategories
NursingStationOptionValuesLog
NursingStationAdminTimesLog
ProgIDs
FeeSchedLog
AdminSchedsLog
FacilityOptionLog
PatContactsLog
AutoMedIds
ASAP2007IDQualifiers
FlowFormatsLog
PharmacyOptionLog
AutoMedIdsLog
InsPlanECSCdsLog
PSFormats
DeliverySigneeTitlesLog
RxAllAuthReqd
AutoExternalMedIdsLog
FacilityOptions
RTSFormatsLog
TIGroupDefinitions
Billing
vRxAuthReqd
ASAP2007Jurisdictions
PharmacyOptions
ASAP2007RelationshipCdsLog
PharmacistFLQueueFacilitiesLog
RiskAssessment
QualityEventReasonDefs
FacilityCustomFieldsLog
PatientPerDiemEligibilityLog
FacilityOptionValues
PBTransactions
AutoPatientIds
PhysicianTIGroups
PassportTransactionIDsLog

DTMSHistory
ASAP2007RelationshipCds
PharmacyOptionValues
NursingStationCyclesLog
QualityEventReasons
HPODetailLog
CustomReports_backup_20220805
CareLvlCdsLog
FacilityRooms
PatDoNotSendItemsLog
HRxPBComponents
ExternalPatientIDs
HRxAdminTimes
ASNFormats
FwHL7InterfacesLog
PharmacyRxChecklistItems
AddlNDCVendors
QRTZ_CALENDARS
InsPlanFormulariesLog
QualityEvents
ExpirationDateByGPI
DeliveryRouteDistances
CompoundIngredModifierCodesLog
customreports_backup_20220808
FacilityTaxStatus
PatNames
FamCustomerNos
SecUserLoginsLog
QRTZ_CRON_TRIGGERS
HRxChecklistItems
Behaviors
PharmacyTeams
ASNFormatsLog
AllowablePharmacies
v0040PatientPrimaryMops
PharmacistsLog
TIGroupDefinitionsLog
QRTZ_FIRED_TRIGGERS
QualityEventTypes
ExpirationDateByCCID
FacilityDocsLog
PatientsLog
FacPackageTypes
v0040PatientSecondaryMOPs
FamIDs
QRTZ_PAUSED_TRIGGER_GRPS
PatientNoteDescriptionsLog
HRxChecklistItemsLog
BlankFormats
PharmacyUserCosts

AutoExternalMedIds
vPatNames
NursingStationGroupsLog
RiskAssessmentLog
QRTZ_SCHEDULER_STATE
QualityEventUsers
HPOHeadersLog
ExpirationDateByGPI
CareLvlLocationsLog
FacPackagingGroupExceptions
PatientAllergiesLog
frm0240View
PatContacts
QRTZ_LOCKS
HRxClarificationCds
Connections
FwInterfacesLog
PharmRxNumbers
CompoundIngredModifierCodes
DTMSHistoryLog
QRTZ_JOB_DETAILS
V0104RxEcsHistory
InsPlanFormularyLog
v0101RxWithPatName
RawBCs
ExpirationDateByCCID
CompoundIngredsLog
Races
FacRoNumbers
PatDoNotSendItems
SecUserProgsLog
PhysicianTIGroupsLog
QRTZ_SIMPLE_TRIGGERS
HRxClinicalWarnings
Control
PODetail
BehaviorsLog
CompoundIngreds
PharmacistTeamsLog
QRTZ_SIMPROP_TRIGGERS
ReturnAdjustmentReasons
FacilityLinkAlertsLog
Ethnicities
PatientsInterfacedLog
FacTypeDefs
v0106BatchAccRejCount
PatientAllergies
QRTZ_BLOB_TRIGGERS
PhProgFormatsLog
HRxCustomFields

FWPCIntUserAccess
CSDLFormats
POHeaders
CompoundPartialReturnValidations
SqlJobs
v0109SecMop
NursingStationPackageTypesLog
QRTZ_TRIGGERS
RTSFormats
InventoryLog
vDeliveryHistory
VaccinationHistory
DefaultMarGroupsLog
GlobalLitOrdAdminTimes
PatientBehaviorsLog
vCommittedInventory
PatientBehaviors
QRTZ_JOB_HISTORY
HRxDirections
CustomBillingExport
GeriMedFilesLog
PrepackLabelPrintLog
Compounds
vSqlJobs
vCommittedInventoryByZoneBin
InsPlanGroupIDsLog
SecurityLog
CompoundPartialReturnValidationsLog
GlobalLitOrds
vToteAssignsAndHistory
PatientCustomerNos
SigCdsLog
InventoryAuditFields
HRxECSFields
VaccinationsLog
CustomFieldDefs
Pricing
BlankFormatsLog
CompoundsAuditLog
vToteAssignsAndHistoryAll
PharmacyCustomFieldsLog
SecUserLogins
FacilityNotesLog
PatientTaxStatusLog
GlobalLitOrdsInterfaced
vToteAssignsAndHistoryAllSP
PatientCustomFields
PdmpQueryResult
PkgLblFormatsLog
HRxIngreds

CustomReportFolders
PricingLog
CompoundsAuditLogFields
PBSplitTransactions
NursingStationsLog
SecUserProgs
InventoryActPkgCostHistLog
DefInvoiceGrpsLog
HFacAdminTimes
PatientCustomerNosLog
PatientDocs
HRxLabels
PendingMedRecLabels
CustomReports
HL7AllergyTranslationsLog
ReconstitutionConcentrations
CompoundTaxStatus
InsPlanOptionCategoriesLog
SigCds
CompoundsLog
HNursingStationAdminTimes
PatientDXs
SigFormatsLog
HRxs
CustomReportSecurity
ReconstitutionDefinitions
DatatracCouriers
PharmacyOptionCategoriesLog
SigFormats
FacilityOptionCategoriesLog
PatientXfersLog
PhTheraChangeLevelsLog
InsFormularyIDs
PatientE1TransactionHistory
POFFormatsLog
LOA
DischargeFormats
Reminders
DatatracSettings
IncompleteDeliveryReasons
PackagingGroupsLog
StateCds
InventoryAvgUnitCostHistLog
DeliveriesLog
InsGroups
PatientCustomFieldsLog
PatientLitOrdAdminTimes
OrderEntryStats
HL7MessagesLog
RxStatIDs

VaccinationProviders
DeliveryAgents
InsPlanOptionLogLog
RxChangeRequestRxs
StateFormularyLicenses
MhaPreRequest
CompoundTaxStatusLog
InsPlanCustomerNos
IncompleteDeliveryReasonsLog
PatientLitOrds
StateCdsLog
InsPlansAuditFields
PackListComments
DiscontinuedMedNotices
TaxAuthorities
VaccinationProvidersLog
PhTheraChangeLevels
ControlLog
DischargeReasons
PharmacyOptionLogLog
StateMedicaidFormats
FacilityOptionLogLog
PatPackagingGroupExceptionsLog
InsPlanECSCds
PatientLitOrdsInterfaced
InventoryZonesAuditFields
RxChangeRequest
PostItLog
PARHistory
ProductLicense
DSFormats
TestClaimHistory
RxPickupsLog
DrugCategories
PatientStatusNamesLog
PreDefinedTextCategories
StatementFormats
InventoryCustomFieldsLog
DrugAuthorizationsLog
PharmacyStateLicenses
InsPlanFormularies
PatientDocsLog
PatientMCareCycles
FacilitiesAuditFields
RxChangeRxRequests
Payments
DURRules
HL7PendingTQDLog
TestClaimRejectCds
DrugCategoryDefs

PreDefinedTexts
InsPlanOptionsLog
SubMenuIds
DatatracCouriersLog
PhTheraChangeLevelEcmFormsLog
EdpUserNpi
PharmacyStateLicensesLog
InsPlanFormulary
PatientMopActiveDates
StateFormularyLicensesLog
PhysiciansAuditFields
RxChangeRequestMedication
Prescriptions
ECMAssociationType
UserAltPharmacies
CSDLFormatsLog
DrugZones
PharmacyOptionsLog
PreDefinedTextCategoriesLog
SystemOptionCategories
FacilityOptionsLog
PatPackagingGroupsLog
EdpUserNpiChanges
InsPlanGroupIDs
PatientMopAdditionalInfo
Stops
PostItActionsLog
ProspectiveBilledRxs
ECMDocumentAssociation
Vendors
ExternalExportIDs
eCourierSettings
PerDiemFormularyLog
RxChangeRequestRxAdminTimes
SystemOptionLog
InventoryPartialReturnValidationsLog
AdditionalOrderMessageFields
ExternalFacilityIDsLog
InsPlanOptionCategories
PatientDXsLog
PatientMopEcsFields
RefillReminders
ECSFields
HL7RouteNamesLog
NsExternalExportIDs
PhTheraChangeLevelEcmForms
ECSHistory
PreDefinedTextsLog
PAConfig
StopsLog

InsPlanOptionValuesLog
RxChangeRequestRxClarificationCds
SystemOptions
DatatracSettingsLog
InsPlanOptionLog
PatientMopPriceMatch
ArchiveQueue
StateMedicaidFormatsLog
RTSWarnings
ECSFieldValues
CustomBillingExportLog
ECSHistoryErrors
PharmacyOptionValuesLog
CustomerGroups
vQRTZ_CURRENT_SCHEDULE
RxChangeRequestRxCustomFields
TSFormats
FacilityOptionValuesLog
ReorderAuthorizationsLog
InsPlanOptions
PatientMopPriceOverrides
PostItCatCdsLog
RxAdminTimes
ECSRejectCds
RxsInterfacedLog
ECSHistoryOpt
PerDiemRatesLog
ArchiveLog
Customers
RxChangeRequestRxDirections
UPSBillOpts
InventoryReturnsLog
ExternalNursingStationIDsLog
PhTheraChangeLevelContactsLog