**IN THE UNITED STATES DISTRICT COURT**
**FOR THE NORTHERN DISTRICT OF ILLINOIS**

LEEROY PERKINS, on behalf of himself and all others similarly situated,

Plaintiff,

v.

COMMONSPIRIT HEALTH,

Defendant.

Case No. _____

**CLASS ACTION COMPLAINT**

**JURY TRIAL DEMANDED**

Plaintiff Leeroy Perkins ("Plaintiff") brings this Class Action Complaint on behalf of himself, and all others similarly situated, against Defendant, CommonSpirit Health ("CommonSpirit" or "Defendant"), alleging as follows based upon information and belief and investigation of counsel, except as to the allegations specifically pertaining to them, which are based on personal knowledge:

## NATURE OF THE ACTION

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

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

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

3. CommonSpirit is the second-largest health system in the United States, operating 140 hospitals and over 1,000 care sites across 21 states.[1]

4. As a healthcare provider, Defendant knowingly obtains sensitive patient PII and PHI and has a resulting duty to securely maintain such information in confidence.

5. On December 1, 2022, CommonSpirit notified its patients at its affiliated entity Virginia Mason Franciscan Health that their PII and PHI stored on its systems had been compromised by a ransomware attack (the "Data Breach").[2]

6. Based on the public statements of Defendant to date, a wide variety of PII and PHI was implicated in the breach, including but not limited to names, addresses, phone numbers, dates of birth, and unique IDs used internally by CommonSpirit of patients, family members of patients, and caregivers of patients.[3]

7. As a direct and proximate result of Defendant's failure to implement and follow basic security procedures, Plaintiff's and Class Members' PII and PHI is now in the hands of cybercriminals.

---

[1] Bill Toulas, *CommonSpirit Health Ransomware Attack Exposed Data of 623,000 Patients*, Bleeping Computer (Dec. 8, 2022), https://www.bleepingcomputer.com/news/security/commonspirit-health-ransomware-attack-exposed-data-of-623-000-patients/.

[2] *CommonSpirit Health Provides Cyberattack Update and Notification of Data Breach Involving Virginia Mason Franciscan health In Washington State*, PR Newswire (Dec. 1, 2022), https://www.prnewswire.com/news-releases/commonspirit-health-provides-cyberattack-update-and-notification-of-data-breach-involving-virginia-mason-franciscan-health-in-washington-state-301691982.html.

[3] *Id.*

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

9. Plaintiff, on behalf of himself, and all others similarly situated, alleges claims for negligence, negligence *per se*, and declaratory judgment. Plaintiff seeks damages and injunctive relief, including the adoption of reasonably sufficient practices to safeguard PII and PHI in Defendant's custody in order to prevent incidents like the Data Breach from reoccurring in the future.

## PARTIES

10. Plaintiff Leeroy Perkins is an adult who, at all relevant times, is a resident and a citizen of the State of Washington. Since approximately 2003, Plaintiff has been a patient of Virginia Mason Franciscan Health, a hospital currently in Defendant's network. Plaintiff received a Data Breach notification informing him that his PII and PHI he provided to Defendant had been compromised in the Data Breach.

11. Since the announcement of the Data Breach, Plaintiff has been required to spend his valuable time monitoring his various accounts and changing his account passwords in an effort to detect and prevent any misuses of his PII and PHI—time which he would not have had to expend but for the Data Breach.

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

13. Defendant CommonSpirit Health is a Colorado not-for-profit corporation with a principal place of business located at 444 W. Lake St. STE 2500, Chicago, IL 60606. Defendant is a citizen of Illinois.

## JURISDICTION AND VENUE

14. This Court has jurisdiction over this action pursuant to 28 U.S.C. § 1332(d)(2)(A), as modified by the Class Action Fairness Act of 2005, because at least one member of the Class, as defined below, is a citizen of a different state than Defendant, there are more than 100 members of the Class, and the aggregate amount in controversy exceeds $5,000,000 exclusive of interests and costs.

15. This Court has personal jurisdiction over Defendant because Defendant maintains its principal place of business in this District.

16. Pursuant to 28 U.S.C. § 1391(b)(1), venue is proper in this District because this is the District in which Defendant resides.

## FACTUAL BACKGROUND

### A. CommonSpirit and the Services It Provides.

17. CommonSpirit touts itself as "one of the largest nonprofit health systems in the U.S., with more than 1,000 care sites in 21 states coast to coast, serving 20 million patients in big cities and small towns across America."[4]

18. In 2021, CommonSpirit acquired Seattle-based Virginia Mason, and combined it with CHI Franciscan to form an integrated health system called Virginia Mason Franciscan

[4] *Building a nation of Healthy Communities*, CommonSpirit, https://www.commonspirit.org/ (last visited Dec. 27, 2022).

Health.[5] Virginia Mason Franciscan Health consists of 11 hospitals and nearly 300 care sites serving western Washington.[6]

19. While providing healthcare services, Defendant receives, creates, and handles PII and PHI, which includes, *inter alia*, patient, family member and caregiver names, addresses, phone numbers, dates of birth, and unique IDs used internally by Defendant.

20. Patients must entrust their PII and PHI to Defendant to receive healthcare services, and in return, they reasonably expect that Defendant will safeguard their highly sensitive information and keep their PHI confidential.

21. Even though CommonSpirit "understand[s] that [patent] protected health information is private and personal" and is "committed to protecting it" [7] it nevertheless employed inadequate data security measures to protect and secure the PII and PHI patients entrusted to it, resulting in the Data Breach and compromise of Plaintiff's and Class Members' PII and PHI.

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

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

23. CommonSpirit also knew that a breach of its systems, and exposure of the information stored therein, would result in the increased risk of identity theft and fraud against the

[5] Tina Reed, CHI Franciscan, *Virginia Mason Finalize Acquisition Deal and Roll Out New Name*, Fierce Healthcare (Jan. 6, 2021), https://www.fiercehealthcare.com/hospitals/chi-franciscan-virginia-mason-finalize-acquisition-deal-and-roll-out-new-name#:~:text=Healthcare%20giant%20CommonSpirit%20Health%20finalized,as%20Virginia%20Mason%20Franciscan%20Healh.

[6] Jacqueline LaPointe, *CHI Franciscan, Virginia Mason Complete Healthcare Merger*, Revcycle Intelligence (Jan. 7, 2021), https://revcycleintelligence.com/news/chi-franciscan-virginia-mason-complete-healthcare-merger.

[7] *Notice of Privacy Practices*, Virginia Mason Franciscan Health, https://www.vmfh.org/content/dam/vmfhorg/pdf/vmfh-npp-english.pdf (last updated June 2022).

individuals whose PII and PHI was compromised, as well as intrusion into their highly private health information.

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

25. PII has considerable value and constitutes an enticing and well-known target to hackers. Hackers easily can sell stolen data as there has been a "proliferation of open and anonymous cybercrime forums on the Dark Web that serve as a bustling marketplace for such commerce."[8] PHI, in addition to being of a highly personal and private nature, can be used for medical fraud and to submit false medical claims for reimbursement.

26. The prevalence of data breaches and identity theft has increased dramatically in recent years, accompanied by a parallel and growing economic drain on individuals, businesses, and government entities in the U.S. In 2021, there were 4,145 publicly disclosed data breaches, exposing 22 billion records. The United States specifically saw a 10% increase in the total number of data breaches.[9]

27. In tandem with the increase in data breaches, the rate of identity theft complaints has also increased over the past few years. For instance, in 2017, 2.9 million people reported some form of identity fraud compared to 5.7 million people in 2021.[10]

---

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

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

[10] *Insurance Information Institute, Facts + Statistics: Identity theft and cybercrime*, Insurance Information Institute, https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime#Identity%20Theft%20And%20Fraud%20Reports,%202015-2019%20 (last visited Dec. 1, 2022).

28. The healthcare industry has become a prime target for threat actors: "High demand for patient information and often-outdated systems are among the nine reasons healthcare is now the biggest target for online attacks."[11]

29. Additionally, "[h]ospitals store an incredible amount of patient data. Confidential data that's worth a lot of money to hackers who can sell it quickly – making the industry a growing target."[12]

30. Indeed, cybercriminals seek out PHI at a greater rate than other sources of personal information. In a 2022 report, the healthcare compliance company Protenus found that there were 905 medical data breaches in 2021, leaving over 50 million patient records exposed for 700 of the 2021 incidents. This is an increase from the 758 medical data breaches that Protenus compiled in 2020.[13]

31. The healthcare sector suffered about 337 breaches in the first half of 2022 alone according to Fortified Health Security's mid-year report released in July. The percentage of healthcare breaches attributed to malicious activity rose more than 5 percentage points in the first six months of 2022 to account for nearly 80 percent of all reported incidents.[14]

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

---

[11] *The healthcare industry is at risk*, SwivelSecure https://swivelsecure.com/solutions/healthcare/healthcare-is-the-biggest-target-for-cyberattacks/ (last visited Dec. 1, 2022).
[12] *Id.*
[13] *2022 Breach Barometer*, PROTENUS, https://www.protenus.com/breach-barometer-report (last visited Dec. 1, 2022).
[14] Jill McKeon, *Health Sector Suffered 337 Healthcare Data Breaches in First Half of Year*, Cybersecurity News (July 19, 2022), available: https://healthitsecurity.com/news/health-sector-suffered-337-healthcare-data-breaches-in-first-half-of-year.

33. As indicated by Jim Trainor, former second in command at the FBI's cyber security division: "Medical records are a gold mine for criminals—they can access a patient's name, DOB, Social Security and insurance numbers, and even financial information all in one place. Credit cards can be, say, five dollars or more where PHI records can go from $20 say up to—we've even seen $60 or $70."[15] A complete identity theft kit that includes health insurance credentials may be worth up to $1,000 on the black market, whereas stolen payment card information sells for about $1.[16]

34. According to Experian:

> Having your records stolen in a healthcare data breach can be a prescription for financial disaster. If scam artists break into healthcare networks and grab your medical information, they can impersonate you to get medical services, use your data open credit accounts, break into your bank accounts, obtain drugs illegally, and even blackmail you with sensitive personal details.
>
> ID theft victims often have to spend money to fix problems related to having their data stolen, which averages $600 according to the FTC. But security research firm Ponemon Institute found that healthcare identity theft victims spend nearly $13,500 dealing with their hassles, which can include the cost of paying off fraudulent medical bills.
>
> Victims of healthcare data breaches may also find themselves being denied care, coverage or reimbursement by their medical insurers, having their policies canceled or having to pay to reinstate their insurance, along with suffering damage to their credit ratings and scores. In the worst cases, they've been threatened with losing custody of their children, been charged with drug trafficking, found it hard to get hired for a job, or even been fired by their employers.[17]

---

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

[16] *Managing cyber risks in an interconnected world, Key findings from The Global State of Information Security® Survey 2015*, PriceWaterhouseCoopers, https://www.pwc.com/gx/en/consulting-services/information-security-survey/assets/the-global-state-of-information-security-survey-2015.pdf (last visited Dec. 1, 2022).

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

35. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches: "[I]n some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the [Dark] Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm."[18]

36. Even if stolen PII or PHI does not include financial or payment card account information, that does not mean there has been no harm, or that the breach does not cause a substantial risk of identity theft. Freshly stolen information can be used with success against victims in specifically targeted efforts to commit identity theft known as social engineering or spear phishing. In these forms of attack, the criminal uses the previously obtained PII and PHI about the individual, such as name, address, email address, and affiliations, to gain trust and increase the likelihood that a victim will be deceived into providing the criminal with additional information.

37. Based on the value of its patients' PII and PHI to cybercriminals, Defendant certainly knew the foreseeable risk of failing to implement adequate cybersecurity measures.

**C. CommonSpirit Breached its Duty to Protect its Patient PII and PHI.**

38. On October 2, 2022, CommonSpirit detected activity on its IT network that it later determined to be ransomware.[19]

[18] U.S. Gov't Accountability Office, Report to Congressional Requesters, Personal Information, June 2007: https://www.gao.gov/new.items/d07737.pdf (last visited Dec. 29, 2022).
[19] *CommonSpirit Health Provides Cyberattack Update and Notification of Data Breach Involving Virginia Mason Franciscan Health in Washington State*, CommonSpirit Health (Dec. 1, 2022), https://www.commonspirit.org/update/notice-of-data-security-incident.

39. On October 4, 2022, CommonSpirit announced that it was managing an IT security issue that was impacting some of its facilities and took certain IT systems, which may have included electronic health records, offline.[20]

40. On October 5, 2022, CommonSpirit announced that it had identified the IT security issue impacting its facilities[21] and later announced on October 17, 2022, that it had been managing a response to a ransomware attack that had impacted some of its facilities.[22]

41. Following the ransomware attack, Defendant engaged third-party experts to investigate the nature and scope of the Data Breach. The investigation determined that between September 16, 2022, and October 3, 2022, an unauthorized third party gained access to portions of CommonSpirit's network, compromising files that contained personal information.[23]

42. The investigation further revealed that the compromised files contained personal information on individuals who received healthcare services in the past, or family members or caregivers of those individuals from Virginia Mason Franciscan Health, an affiliated entity of CommonSpirit.[24]

43. The nature of the information compromised in the Data Breach includes names, addresses, phone numbers, dates of birth, and unique IDs used internally by the organization.[25]

---

[20] *CommonSpirit Update*, CommonSpirit Health (Oct. 4, 2022), https://www.commonspirit.org/update/10-4-2022.

[21] *CommonSpirit Update*, CommonSpirit Health (Oct. 5, 2022), https://www.commonspirit.org/update/10-5-2022.

[22] *CommonSpirit Update*, CommonSpirit Health (Oct. 17, 2022), https://www.commonspirit.org/update/10-17-2022.

[23] *CommonSpirit Health Provides Cyberattack Update and Notification of Data Breach Involving Virginia Mason Franciscan Health in Washington State*, CommonSpirit Health (Dec. 1, 2022), https://www.commonspirit.org/update/notice-of-data-security-incident.

[24] *Id.*

[25] *Id.*

44. On December 1, 2022, approximately two months after first discovering the Data Breach, Defendant reported the Data Breach to the Department of Health and Human Services Office for Civil Rights ("HHS").[26]

45. All in all, more than 623,000 individuals had their PII and/or PHI breached.[27]

46. The Data Breach occurred as a direct result of Defendant's failure to implement and follow basic security procedures, and its failure to follow its own policies, in order to protect its patients' PII and PHI.

47. On or about the same date that Defendant reported the Data Breach to HHS, Defendant provided notice to Plaintiff indicating that his PII and PHI may have been compromised or accessed during the Data Breach.

48. Like Plaintiff, the Class Members received similar notices informing them that their PII and/or PHI was exposed in the Data Breach.

**D. CommonSpirit is Obligated Under HIPAA to Safeguard Personal Information.**

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

50. CommonSpirit is an entity covered by under HIPAA, which sets minimum federal standards for privacy and security of PHI.

51. 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.

---

[26] *Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information*, U.S. Dep't of Health & Human Services, https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (last visited Dec. 28, 2022).
[27] *Id.*

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

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

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

55. 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."[28]

56. While HIPAA permits healthcare providers to disclose PHI to third parties under certain circumstances, HIPAA does not permit healthcare providers to disclose PHI to

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

cybercriminals nor did Plaintiff or the Class Members consent to the disclosure of their PHI to cybercriminals.

57. As such, CommonSpirit is required under HIPAA to maintain the strictest confidentiality of Plaintiff's and Class Members' PHI that it requires, receives, and collects, and Defendant is further required to maintain sufficient safeguards to protect that information from being accessed by unauthorized third parties.

58. Given the application of HIPAA to CommonSpirit, and that Plaintiff and Class Members entrusted their PHI to Defendant in order to receive healthcare services, Plaintiff and Class Members reasonably expected that Defendant would safeguard their highly sensitive information and keep their PHI confidential.

## E. FTC Guidelines Prohibit CommonSpirit from Engaging in Unfair or Deceptive Acts or Practices.

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

60. The FTC has promulgated numerous guides for businesses that highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[29]

61. The FTC provided cybersecurity guidelines for businesses, advising that businesses should protect personal customer information, properly dispose of personal information that is no

[29] *Start with Security – A Guide for Business*, United States Federal Trade Comm'n (2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf.

longer needed, encrypt information stored on networks, understand their network's vulnerabilities, and implement policies to correct any security problems.[30]

62. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to private data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.[31]

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

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

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

---

[30] *Protecting Personal Information: A Guide for Business*, United States Federal Trade Comm'n, https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personalinformationpdf.

[31] *Id.*

**F. Plaintiff and Class Members Suffered Damages.**

66. For the reasons mentioned above, Defendant's conduct, which allowed the Data Breach to occur, caused Plaintiff and members of the Class significant injuries and harm in several ways. Plaintiff and members of the Class must immediately devote time, energy, and money to: 1) closely monitor their medical statements, bills, records, and credit and financial accounts; 2) change login and password information on any sensitive account even more frequently than they already do; 3) more carefully screen and scrutinize phone calls, emails, and other communications to ensure that they are not being targeted in a social engineering or spear phishing attack; and 4) search for suitable identity theft protection and credit monitoring services, and pay to procure them.

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

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

69. From a recent study, 28% of consumers affected by a data breach become victims of identity fraud—this is a significant increase from a 2012 study that found only 9.5% of those affected by a breach would be subject to identity fraud. Without a data breach, the likelihood of identify fraud is only about 3%.[32]

[32] Stu Sjouwerman, *28 Percent of Data Breaches Lead to Fraud*, KnowBe4, https://blog.knowbe4.com/bid/252486/28-percent-of-data-breaches-lead-to-fraud (last visited Dec. 1, 2022).

70. With respect to health care breaches, another study found "the majority [70%] of data impacted by healthcare breaches could be leveraged by hackers to commit fraud or identity theft."[33]

71. "Actors buying and selling PII and PHI from healthcare institutions and providers in underground marketplaces is very common and will almost certainly remain so due to this data's utility in a wide variety of malicious activity ranging from identity theft and financial fraud to crafting of bespoke phishing lures."[34]

72. The reality is that cybercriminals seek nefarious outcomes from a data breach and "stolen health data can be used to carry out a variety of crimes."[35]

73. Health information in particular is likely to be used in detrimental ways—by leveraging sensitive personal health details and diagnoses to extort or coerce someone, and serious and long-term identity theft.[36]

74. "Medical identity theft is a great concern not only because of its rapid growth rate, but because it is the most expensive and time consuming to resolve of all types of identity theft. Additionally, medical identity theft is very difficult to detect which makes this form of fraud extremely dangerous."[37]

---

[33] Jessica David, *70% of Data Involved in Healthcare Breaches Increases Risk of Fraud*, HealthITSecurity, https://healthitsecurity.com/news/70-of-data-involved-in-healthcare-breachesincreases-risk-of-fraud (last visited Dec. 1, 2022).
[34] *Id.*
[35] Andrew Steger, *What Happens to Stolen Healthcare Data?*, HealthTech (Oct. 30, 2019), https://healthtechmagazine.net/article/2019/10/what-happens-stolen-healthcare-data-perfcon.
[36] *Id.*
[37] *The Potential Damages and Consequences of Medical Identity theft and Healthcare Data Breaches*, Experian, https://www.experian.com/assets/data-breach/white-papers/consequences-medical-id-theft-healthcare.pdf (last visited Dec. 1, 2022).

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

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

## CLASS ALLEGATIONS

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

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

> All individuals in the United States whose PII and/or PHI was compromised in the CommonSpirit Data Breach which was announced on or about December 1, 2022 (the "Class").

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

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

81. **Numerosity:** Plaintiff is informed and believes, and thereon alleges, that there are at minimum, thousands of members of the Class described above. The exact size of the Class and

the identities of the individual members are identifiable through Defendant's records, including but not limited to the files implicated in the Data Breach, but based on public information, the Class includes approximately 623,000 individuals.

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

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

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

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

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

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

84. **Adequacy of Representation:** Plaintiff is an adequate representative of the Class because his interests do not conflict with the interests of the members of the Class. Plaintiff will fairly, adequately, and vigorously represent and protect the interests of the members of the Class and has no interests antagonistic to the members of the Class. In addition, Plaintiff has retained

counsel who are competent and experienced in the prosecution of class action litigation. The claims of Plaintiff and the Class Members are substantially identical as explained above.

85. **Superiority:** This class action is appropriate for certification because class proceedings are superior to other available methods for the fair and efficient adjudication of this controversy and joinder of all members of the Class is impracticable. This proposed class action presents fewer management difficulties than individual litigation, and provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single court. Class treatment will create economies of time, effort, and expense, and promote uniform decision-making.

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

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

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

**FIRST CAUSE OF ACTION**
**NEGLIGENCE**
**(On Behalf of Plaintiff and the Class)**

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

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

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

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

93. Defendant's duty also arose from Defendant's position as a healthcare provider. Defendant holds itself out as a trusted provider of healthcare, and thereby assumes a duty to reasonably protect its patients' information. Indeed, Defendant was in a unique and superior position to protect against the harm suffered by Plaintiff and Class Members as a result of the Data Breach.

94. Defendant breached the duties owed to Plaintiff and Class Members and thus was negligent. As a result of a successful attack directed towards Defendant that compromised Plaintiff's and Class Members' PII and PHI, Defendant breached its duties through some

combination of the following errors and omissions that allowed the data compromise to occur: (a) mismanaging its system and failing to identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of patient information that resulted in the unauthorized access and compromise of PII and PHI; (b) mishandling its data security by failing to assess the sufficiency of its safeguards in place to control these risks; (c) failing to design and implement information safeguards to control these risks; (d) failing to adequately test and monitor the effectiveness of the safeguards' key controls, systems, and procedures; (e) failing to evaluate and adjust its information security program in light of the circumstances alleged herein; (f) failing to detect the breach at the time it began or within a reasonable time thereafter; (g) failing to follow its own privacy policies and practices published to its patients; and (h) failing to adequately train and supervise employees and third party vendors with access or credentials to systems and databases containing sensitive PII or PHI.

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

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

a. Theft of their PII and/or PHI;

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

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

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

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

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

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

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

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

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

**SECOND CAUSE OF ACTION**
**NEGLIGENCE PER SE**
**(On Behalf of Plaintiff and the Class)**

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

99. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce" including, as interpreted and enforced by the FTC, the unfair act or practice by entities such as Defendant or failing to use reasonable measures to protect PII and PHI. Various FTC publications and orders also form the basis of Defendant's duty.

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

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

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

103. Defendant is an entity covered under HIPAA which sets minimum federal standards for privacy and security of PHI.

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

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

106. Defendant violated HIPAA by actively disclosing Plaintiff's and the Class Members' electronic PHI and by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' PHI.

107. Plaintiff and the Class Members are patients within the class of persons HIPAA was intended to protect.

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

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

110. As a direct and proximate result of Defendant's negligence, Plaintiff's and Class Members have been injured as described herein and in Paragraph 96 above, and are entitled to damages, including compensatory, punitive, and nominal damages, in an amount to be proven at trial.

## THIRD CAUSE OF ACTION
## DECLARATORY JUDGMENT
## (On Behalf of Plaintiff and the Class)

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

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

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

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

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

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

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

116. If an injunction is not issued, Plaintiff will suffer irreparable injury, and lack an adequate legal remedy, in the event of another data breach at Defendant. The risk of another such

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

117. The hardship to Plaintiff if an injunction is not issued exceeds the hardship to Defendant if an injunction is issued. Plaintiff will likely be subjected to substantial identity theft and other damage. On the other hand, the cost to Defendant of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Defendant has a pre-existing legal obligation to employ such measures.

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

## PRAYER FOR RELIEF

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

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

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

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

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

e. Declaratory and injunctive relief as described herein;

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

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

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

**JURY TRIAL DEMAND**

A jury trial is demanded on all claims so triable.

Dated: December 29, 2022

Respectfully submitted,

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

*Counsel for Plaintiff*