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

JOSE ANTONIO KOCH, *individually and on behalf of minor John Doe, minor James Doe, and all others similarly situated*, Plaintiffs, v. COMMONSPIRIT HEALTH, Defendant.	Case No. _____ **CLASS ACTION COMPLAINT** **JURY DEMAND**

CLASS ACTION COMPLAINT

Plaintiffs Jose Antonio Koch, individually on behalf of minors John and James Doe ("Plaintiffs") and all others similarly situated, brings this class action lawsuit against CommonSpirit Health ("CommonSpirit" or "Defendant") to obtain damages, restitution and injunctive relief for the Class, as defined herein. Plaintiffs set forth the following allegations upon information and good faith belief, except as to their own actions, the investigation of their counsel and certain facts that are a matter of public record.

NATURE OF THE ACTION

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

2. In 2021, CommonSpirit acquired Seattle-based Virginia Mason, and combined it with CHI Franciscan to form an integrated health system called Virginia Mason Franciscan Health.[2]

[1] https://www.commonspirit.org/who-we-are/our-locations (last accessed Jan. 8, 2023).
[2] https://www.fiercehealthcare.com/hospitals/chi-franciscan-virginia-mason-finalize-acquisition-deal-and-roll-out-new-name (last accessed Jan. 8, 2023). Virginia Mason Franciscan Health consists of 11 hospitals and nearly 300 care sites serving western Washington. https://revcycleintelligence.com/news/chi-franciscan-

3. As detailed herein, CommonSpirit failed to properly secure and to safeguard individuals' personally identifiable information ("PII") and non-public personal health information ("PHI")[3] including, but not limited to, their names, addresses, phone numbers, dates of birth, and unique IDs used internally by the Defendant - despite its duty to protect this highly sensitive data.[4]

4. For more than two weeks, between September 16, 2022, and October 3, 2022, CommonSpirit lost control of the highly sensitive Private Information and as a result of a data breach perpetrated by an unauthorized party which gained access to Defendant's computer system through a ransomware attack (the "Data Breach").[5]

5. CommonSpirit has ***not*** been forthcoming about the Data Breach, which affected ***at least*** 623,774 individuals, ***at least*** 7 hospitals and potentially 300 medical care sites managed by Defendant.[6]

6. On December 1, 2022, nearly two and a half months after the Data Breach began, CommonSpirit first disclosed the Data Breach to federal authorities[7] and began notifying affected individuals at its affiliated entity Virginia Mason Franciscan Health that their PII and PHI stored on its systems had been compromised by a ransomware attack.[8]

---

virginia-mason-complete-healthcare-merger (last accessed Jan. 8, 2023).

[3] This information is collectively referred to as "PII and PHI" or collectively, "Private Information."

[4] *See* https://www.commonspirit.org/update/notice-of-data-security-incident (individuals affected include Defendant's patients, family members of patients, and/or caregivers of patients) (last accessed Jan. 8, 2023).

[5] *See* https://www.commonspirit.org/update/notice-of-data-security-incident; https://www.fiercehealthcare.com/health-tech/aha-himss-health-it-players-reveal-lessons-commonspirit-attack (last accessed January 10, 2023).

[6] *See* https://www.commonspirit.org/update/notice-of-data-security-incident; https://revcycleintelligence.com/news/chi-franciscan-virginia-mason-complete-healthcare-merger (last accessed Jan. 8, 2023).

[7] *See* HHS OCR Data Breach Portal, https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (last accessed Jan. 9, 2023).

[8] *See* Notice of Security Incident provided by CommonSpirit (the "Notice"), attached as **Exhibit A** hereto.

7. Despite CommonSpirit reporting only that Virginia Mason Franciscan Health entities have been affected by the data breach, other medical systems in Defendant's system have experienced significant disruptions in their operations which included doctors giving patients wrong doses of medication and patients not being able to schedule appointments.[9]

8. In fact, the number of actual victims of the Data Breach may be much higher – potentially as high as twenty million individuals.[10]

9. While the intrusion of Defendant's systems began in the middle of September 2022, Common Spirit did not manage to detect unusual activity on its IT network until October 2, 2022. CommonSpirit inexplicably waited another month after that—until December 1, 2022 the earliest—to begin to issue notice to affected persons and to notify the authorities.

10. Despite the prevalence of ransomware and other data security attacks in recent years, the Data Breach was a direct result of Defendant's abject failure to implement and to maintain adequate and reasonable cybersecurity procedures and protocols necessary to protect

---

[9] *See* https://www.fiercehealthcare.com/health-tech/aha-himss-health-it-players-reveal-lessons-commonspirit-attack ("Subsidiaries that reported being affected by the attack include CHI Health facilities in Nebraska and Tennessee, Seattle-based Virginia Mason Franciscan Health providers, MercyOne Des Moines Medical Center, Houston-based St. Luke's Health and Michigan-based Trinity Health System. Full access in CHI Memorial's MyChat system and outpatient locations has yet to be recovered. It is unclear how extensively the ransomware attack affected all centers for medical care"); https://www.cybertalk.org/2022/11/17/ransomware-attack-on-commonspirit-health-could-affect-20-million-americans/ (report of doctor informing caretaker that her minor son was given the wrong dose of medicine at Defendant's MercyOne Des Moines Medical Center after the hospital's systems were taken offline as a result of the Data Breach); https://www.3newsnow.com/news/local-news/chi-health-dealing-with-it-security-issue-leaving-local-patients-unable-to-schedule-appointments (IT issues apparently caused by the Data Breach preventing patients from making new appointments) (last accessed Jan. 8, 2023).

[10] *See* https://thehipaaetool.com/commonspirit-cyber-attack-affects-millions/#:~:text=CommonSpirit%20Cyber%20Attack%20Affects%20Millions%20November%2015%2C%202022,than%20a%20month%20after%20it%20was%20first%20reported (stating that "[***m**ore than 20 million patients have been victimized by a ransomware attack on CommonSpirit Health*. This is the second largest healthcare data breach in history and is still unfolding more than a month after it was first reported") (emphasis added). CommonSpirit admits that its "review of the [compromised] files is ongoing." https://www.commonspirit.org/update/notice-of-data-security-incident (last accessed Jan. 8, 2023).

Plaintiffs' and the Class Members' Private Information.

11. The nature of the cyberattacks and potential for improper disclosure of Plaintiffs' and Class Members' Private Information was a known and foreseeable risk to Defendant and thus Defendant was on—at least, constructive—notice that failing to take steps necessary to secure the Private Information from those risks left the information in an extremely dangerous and needlessly vulnerable condition.

12. Defendant disregarded the rights of Plaintiffs and the Class Members by, *inter alia*, (i) intentionally, willfully, recklessly or negligently failing to take adequate and reasonable measures to ensure its data systems were protected against unauthorized intrusions; (ii) failing to disclose that it did not have adequately robust computer systems and security practices to safeguard Class Members' PII and PHI; (iii) failing to take standard and reasonably available steps to prevent the Data Breach, and (iv) failing to provide Plaintiffs and the Class Members with a prompt, complete and accurate notice of the Data Breach.

13. Plaintiffs' and the putative Class Members' identities are now at risk because of Defendant's conduct since the Private Information that Defendant obtained and maintained is now in the hands of data thieves.

14. As a result of the Data Breach, Plaintiffs and Class Members have been exposed to a heightened and imminent risk of fraud, financial identity theft, and medical identity theft.

15. Plaintiffs and Class Members must now and in the future closely monitor ***all*** of their financial and health information and accounts to guard against fraud and identity theft. Plaintiffs and Class Members may also incur out of pocket costs for, *e.g.*, purchasing credit monitoring services, credit freezes, credit reports or other protective measures to detect and to deter such identity theft.

16. Since the announcement of the Data Breach, Plaintiffs had been required to spend

their valuable time monitoring their various accounts and changing their account passwords in an effort to detect and prevent any misuses of their PII and PHI—time which they would not have had to expend but for the Data Breach.

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

18. Plaintiffs therefore bring this class action lawsuit on behalf of all those similarly situated to address Defendant's inadequate safeguarding of Class Members' Private Information, and for failing to provide timely and adequate notice to Plaintiffs and Class Members that their Private Information had been subject to the unauthorized access of an unknown third party and to specify the types of information accessed.

19. Plaintiffs seek remedies including, but not limited to, compensatory damages, reimbursement of out-of-pocket costs, and injunctive relief including improvements to Defendant's data security systems, future annual audits, and adequate credit monitoring services funded by Defendant.

PARTIES

20. Plaintiffs are, and were at all relevant times, individual citizens residing in Kitsap County in the State of Washington. Plaintiffs received Data Breach Notices informing them that the PII and PHI they provided to Defendant, including their names, addresses, phone numbers, dates of birth, and unique IDs used internally by Defendant, had been compromised in the Data Breach.

21. 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, Illinois. Defendant is a citizen of Illinois.

JURISDICTION AND VENUE

22. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2) ("CAFA") as the amount in controversy exceeds $5 million, exclusive of interest and costs and, upon information and good faith belief based on Defendant's public representations, the number of affected individuals is at least 623,774, many, if not most, of whom have different citizenship from Defendant.

23. This Court has personal jurisdiction over Defendant because it transacts business, contracts to supply services and has caused tortious injury by act or omission with the State of Illinois. In addition, Defendant has its principal place of business located at 444 W. Lake St. STE 2500, Chicago, Illinois, and the computer systems implicated in this Data Breach - as well as the high-level officers who direct, control and coordinate Defendant's activities, including major policy decisions - are likely based in this District. By and through its business operations in this judicial district, Defendant intentionally avails itself of the markets within this judicial district so as to render the exercise of jurisdiction by this Court just and proper.

24. Venue is proper pursuant to 28 U.S.C. § 1391(a)(1) because Defendant is resident in this District, maintains the Private Information at issue in this lawsuit in this District and has caused harm to Class Members residing in this District. Venue is therefore appropriate because a substantial portion of the events giving rise to this action occurred in this District.

STATEMENT OF FACTS

A. The Data Breach.

25. Starting on or about September 16, 2022 and continuing to until at least October 3, 2022, CommonSpirit lost control over Plaintiffs' and the putative Class Members' Private Information when cybercriminals accessed patients' and other individuals' files on Defendant's computer systems via a ransomware attack.

26. Even though the intrusion began on or about September 16, 2022, it was not until two and a half months later that CommonSpirit began to notify the authorities and issue notice to affected victims.

27. According to the Notice of Security Incident, Private Information exposed in the Data Breach included, among other things: names, addresses, phone numbers, dates of birth, and unique IDs used internally by CommonSpirit of patients, family members of patients, and caregivers of patients.[11]

28. The information provided in the Notice and on the U.S. Department of Health and Human Services Office for Civil Rights Data Breach Portal regarding the Data Breach is noticeably scant.[12]

29. Defendant's Notice does not indicate what entity attacked it or whether its system was encrypted or otherwise secured in any fashion prior to the attack.[13]

30. Defendant declines to name a single specific thing that it did other than wait more than two months to begin to provide notice.

31. Defendant's Notice attempts to minimize the extent of harm to Plaintiffs and Class

---

[11] *See* **Exhibit A**.
[12] *Id.*; *see also* https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf.
[13] *See* **Exhibit A**.

Members by stating that an unnamed "unauthorized third party ***may have*** gained access to certain files" including those which contained personal information, and "***some of this data*** was associated with services provided by [certain Defendant's affiliates]" (emphasis added).[14]

32. Defendant does not discuss why it took more than two months from the date of the Data Breach to begin to issue notice.[15]

33. The reason that CommonSpirit is being less than forthcoming is because the Data Breach was a direct result of its failure to implement adequate and reasonable cybersecurity procedures and protocols necessary to protect Plaintiffs' and Class Members' Private Information.

B. Defendant's Responsibility to Safeguard Information.

34. Defendant provides medical services at more than 1,000 care sites and 140 hospitals in more than 21 states across the U.S., making it the second-largest non-profit hospital system in the country.[16]

35. In the course of doing business, CommonSpirit collects very sensitive information about its patients including their Private Information.

36. This sensitive information is provided by patients to Defendant for healthcare related services.

37. Defendant is required by law to maintain the privacy and security of patients' protected health information.

38. CommonSpirit owed Plaintiffs and Class Members a duty to safeguard their Private Information.

---

[14] *Id*.

[15] CommonSpirit is being purposefully evasive about the information conveyed because it is more concerned with trying to limit its exposure than it is providing complete and accurate information to almost 700 thousand persons affected by this Data Breach so that they can take preventative and/or precautionary measures.

[16] *See* https://www.commonspirit.org/who-we-are/our-locations (last accessed Jan. 8, 2023).

39. First, CommonSpirit owed a duty to safeguard Private Information pursuant to a number of statutes, including the Health Insurance Portability and Accountability Act ("HIPAA") and the Federal Trade Commission Act ("FTC Act"), to ensure that all information it collected and stored was secure. These statutes were intended to protect Plaintiffs and Class Members from the type of conduct by CommonSpirit alleged herein.

40. The patient information held by Defendant in its computer systems included the Private Information of Plaintiffs and Class Members. Defendant voluntarily assumed custody of Plaintiffs' and Class Members' PII and PHI for its own profit. Defendant was aware of its obligations, particularly with respect to patient PHI.

41. Next, CommonSpirit owed a duty to safeguard Private Information as it was on notice that it was maintaining highly-valuable data for which it knew there was a risk that it would be targeted by cybercriminals. Defendant knew of the extensive harm that would occur if Plaintiffs' and Class Members' Private Information were exposed through a Data Breach, and thus owed a duty to safeguard that information.

42. Unauthorized disclosure of Plaintiffs' and Class Members' PHI and PII in this Data Breach was not for any legitimate purpose.

43. It is likely that the Data Breach was targeted at the Defendant due to its status as a healthcare entity that collects, creates, and maintains both PII and PHI.

44. Upon information and belief, the targeted Data Breach was expressly designed to gain access to private and confidential data, including (among other things) the PII and PHI of patients like Plaintiffs and Class Members.

45. Because of the Defendant's failure to properly safeguard Plaintiffs' and Class Members' Private Information, data thieves were able to gain unauthorized access to Defendant's computer systems and were able to compromise, access, and acquire the protected Private

Information of Plaintiffs and Class Members.

46. Defendant had obligations created by HIPAA, the FTC, industry standards, state and common law, and its own promises and representations made to Plaintiffs and Class Members to keep their Private Information confidential and to protect it from unauthorized access and disclosure.

47. Given the sensitive nature of the Private Information, CommonSpirit knew that hackers and cybercriminals would be able to commit identity theft, financial fraud, phishing, socially-engineered attacks, healthcare fraud, and other identity-related fraud if they were able to exfiltrate that data from Defendant's servers.

48. CommonSpirit also knew that individuals whose Private Information was stored on its servers would be reasonable in spending time and effort to mitigate their damages and prevent identity theft and fraud if that data were exfiltrated.

49. Defendant's data security obligations were particularly important and should have been apparent given the substantial increase in cyberattacks and/or data breaches in the healthcare industry preceding the date of the breach.

C. Prevalence of Cyber Attacks in Recent Years.

50. Data breaches, including ransomware attacks, are extremely commonplace.

51. In 2021, a record 1,862 data breaches occurred, resulting in approximately 293,927,708 sensitive records being exposed, a 68% increase from 2020.[17]

52. Of the 1,862 recorded data breaches, 330 of them, or 17.7% were in the medical or healthcare industry.[18]

---

[17] *See* 2021 Data Breach Annual Report, at 6 (ITRC, Jan. 2022), available at https://www.wsav.com/wp-content/uploads/sites/75/2022/01/20220124_ITRC-2021-Data-Breach-Report.pdf (last accessed Jan. 10, 2023).

[18] *Id.*

53. The 330 breaches reported in 2021 exposed nearly 30 million sensitive records, compared to only 306 breaches that exposed nearly 10 million sensitive records in 2020.[19]

54. 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.[20]

55. In light of recent high profile cybersecurity incidents at other healthcare partner and provider companies, Defendant knew or should have known that its electronic records would be targeted by cybercriminals.

56. Indeed, cyberattacks have become so notorious that the Federal Bureau of Investigation ("FBI") and U.S. Secret Service have issued a warning to potential targets so they are aware of, and prepared for, a potential attack.

57. As one report explained, "[e]ntities like smaller municipalities and hospitals are attractive to ransomware criminals . . . because they often have lesser IT defenses and a high incentive to regain access to their data quickly."[21]

58. In fact, according to the cybersecurity firm Mimecast, 90% of healthcare organizations experienced cyberattacks in the past year.[22]

59. Therefore, the increase in such attacks, and attendant risk of future attacks, was widely known to the public and to anyone in Defendant's industry, including Defendant.

---

[19] *Id.*

[20] *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 Jan. 13, 2023).

[21] FBI, Secret Service Warn of Targeted Ransomware, Law360 (Nov. 18, 2019), https://www.law360.com/articles/1220974 (last accessed Jan. 10, 2023).

[22] *See* Maria Henriquez, Iowa City Hospital Suffers Phishing Attack, Security Magazine (Nov. 23, 2020), https://www.securitymagazine.com/articles/93988-iowa-city-hospital-suffers-phishing-attack (last accessed Jan. 10, 2023).

D. CommonSpirit Acquires, Collects and Stores Class Members' Private Information.

60. As noted above, CommonSpirit is the second-largest nonprofit hospital chain in the U.S..

61. In the course of providing these services, CommonSpirit acquires, collects and stores a massive amount of Private Information.

62. By obtaining, collecting, and using Class Members' Private Information, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiffs' and Class Members' Private Information from access and disclosure.

E. Defendant Knew the Value of Private Information and the Effects of Unauthorized Disclosure.

63. Defendant was (or certainly should have been) well-aware that the Private Information it collects is highly sensitive and of significant value to those who would use it for wrongful purposes.

64. Simply put, Private Information is an extremely valuable commodity to identity thieves.

65. As the FTC recognizes, with PII and PHI identity thieves can commit an array of crimes including identity theft, medical, and tax, credit and bank fraud.

66. Indeed, a robust "cyber black market" exists in which criminals openly post stolen Private Information on multiple underground Internet websites.

67. Indeed, when compromised, healthcare related data is among the most sensitive and personally consequential. A report focusing on healthcare breaches found that the "average total cost to resolve an identity theft-related incident . . . came to about $20,000," and that the victims were often forced to pay out-of-pocket costs for healthcare they did not receive in order to

restore coverage.[23] 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 customers were never able to resolve their identity theft at all. Data breaches and resulting identity theft have a crippling effect on individuals and detrimentally impact the economy as a whole.[24]

68. The ramifications of Defendant's failure to keep Plaintiffs' and Class Members' Private Information secure are long lasting and severe:

> Medical identity theft offers thieves a long-term income. If someone applies for credit in your name, chances are, you'll quickly notice — especially if you have alerts set up through an identity protection service.
>
> But it can take years for victims of medical identity theft to realize they've been targeted. Often, you won't know until you visit the doctor's office or need urgent treatment at the hospital.
>
> By then, a fraudster could have racked up thousands of dollars in fraudulent claims and hit your benefit limit.[25]

69. Once Private Information is stolen, fraudulent use of that information and damage to victims may continue for years.

70. As explained by the Federal Bureau of Investigation, "[p]revention is the most effective defense against ransomware and it is critical to take precaution for protection."[26]

71. To prevent and detect ransomware attacks, including the ransomware attack that resulted in the Data Breach, Defendant could and should have implemented, as recommended by

---

[23] Elinor Mills, *Study: Medical identity theft is costly for victims*, CNET (March 3, 2010), https://www.cnet.com/news/privacy/study-medical-identity-theft-is-costly-for-victims/ (last accessed Jan. 13, 2023).

[24] *Id.*

[25] https://www.aura.com/learn/medical-identity-theft (last accessed Jan. 10, 2023).

[26] *See How to Protect Your Networks from RANSOMWARE*, FBI (2016), https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf (last accessed Jan. 13, 2023).

the United States Government, the following measures:

· Implement an awareness and training program. Because end users are targets, employees and individuals should be aware of the threat of ransomware and how it is delivered.

· Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate 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.

· Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.

· Configure firewalls to block access to known malicious IP addresses.

· Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system.

· Set anti-virus and anti-malware programs to conduct regular scans automatically.

· Manage 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.

· Configure 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.

· Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office

files transmitted via email instead of full office suite applications.

· Implement 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.

· Consider disabling Remote Desktop protocol (RDP) if it is not being used.

· Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.

· Execute operating system environments or specific programs in a virtualized environment.

· Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.

72. To prevent and detect ransomware attacks, including the ransomware attack that resulted in the Data Breach, Defendant could and should have implemented, as recommended by the United States Government, the following measures:

· **Update and patch your computer.** Ensure your applications and operating systems (OSs) have been updated with the latest patches. Vulnerable applications and OSs are the target of most ransomware attacks . . .

· **Use caution with links and when entering website addresses.** Be careful when clicking directly on links in emails, even if the sender appears to be someone you know. Attempt to independently verify website addresses (e.g., contact your organization's helpdesk, search the internet for the sender organization's website or the topic mentioned in the email). Pay attention to the website addresses you click on, as well as those you enter yourself.

> Malicious website addresses often appear almost identical to legitimate sites, often using a slight variation in spelling or a different domain (e.g., .com instead of .net) . . .
>
> · **Open email attachments with caution.** Be wary of opening email attachments, even from senders you think you know, particularly when attachments are compressed files or ZIP files.
>
> · **Keep your personal information safe.** Check a website's security to ensure the information you submit is encrypted before you provide it . . .
>
> · **Verify email senders.** If you are unsure whether or not an email is legitimate, try to verify the email's legitimacy by contacting the sender directly. Do not click on any links in the email. If possible, use a previous (legitimate) email to ensure the contact information you have for the sender is authentic before you contact them.
>
> · **Inform yourself.** Keep yourself informed about recent cybersecurity threats and up to date on ransomware techniques. You can find information about known phishing attacks on the Anti-Phishing Working Group website. You may also want to sign up for CISA product notifications, which will alert you when a new Alert, Analysis Report, Bulletin, Current Activity, or Tip has been published.
>
> **Use and maintain preventative software programs.** Install antivirus software, firewalls, and email filters—and keep them updated—to reduce malicious network traffic . . .[27]

73. To prevent and detect ransomware attacks, including the ransomware attack that resulted in 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 the latest security updates

[27] *See Security Tip (ST19-001) Protecting Against Ransomware*, Cybersecurity & Infrastructure Security Agency (Apr. 11, 2019), https://us-cert.cisa.gov/ncas/tips/ST19-001 (last accessed Jan. 13, 2023).

- Use threat and vulnerability management
- Perform regular audit; remove privilege 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].[28]

74. These are basic, common-sense security measures that every business, not only healthcare businesses, should be doing. CommonSpirit, with its heightened standard of care,

[28] *See Human-operated ransomware attacks: A preventable disaster*, Microsoft (Mar. 5, 2020), https://www.microsoft.com/en-us/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/ (last accessed Jan. 13, 2023).

should be doing even more. By adequately taking these common-sense measures, Defendant could have prevented this Data Breach from occurring.

75. At all relevant times, Defendant knew or reasonably should have known of the importance of safeguarding Private Information and of the foreseeable consequences if its data security systems were breached, including, but not limited to, the significant costs that would be imposed on its healthcare provider clients and, most importantly, on their patients.

76. Defendant breached its obligations to Plaintiffs and Class Members and/or was otherwise negligent and reckless because it failed to properly maintain and to safeguard the computer systems and data that held the stolen Private Information.

77. Defendant's unlawful conduct includes, but is not limited to, the following acts and/or omissions:

a. Failing to maintain an adequate data security system to reduce the risk of data breaches and cyber-attacks;

b. Failing to adequately protect patients' Private Information;

c. Failing to properly monitor the data security systems for existing intrusions; and

d. Failing to ensure that its agents and service providers with access to Plaintiffs' and Class Members' PII and PHI employed reasonable security procedures.

F. Defendant Did Not Comply with FTC Guidelines.

78. The Federal Trade Commission has promulgated numerous guides for businesses which 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]

[29] Federal Trade Commission, *Start With Security*, available at https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last accessed Jan. 10, 2023).

79. In 2016, the FTC updated its publication, *Protecting Private Information: A Guide for Business*, which established cyber-security guidelines for businesses.[30]

80. The guidelines note that businesses should (i) protect the personal customer information that they keep; (ii) properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; (iii) understand their network's vulnerabilities; and (iv) implement policies to correct any security problems.

81. The guidelines also recommend that businesses (i) use an intrusion detection system to discover a breach as soon as it occurs, (ii) monitor all incoming traffic for activity indicating someone is attempting to hack the system, (iii) watch for large amounts of data being transmitted from the system and (iv) have a response plan ready in the event of a breach.[31]

82. The FTC further recommends that companies (i) not maintain PII and/or PHI longer than is needed; (ii) limit access to sensitive data; (iii) require complex passwords to be used on networks; (iv) use industry-tested methods for security; (v) monitor for suspicious activity on the network and (vi) verify that third-party service providers have implemented reasonable security measures.

83. 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 Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45.

84. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

---

[30] https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business (last accessed Jan. 10, 2023).

[31] *Id.*

85. These FTC enforcement actions include actions against healthcare related providers like Defendant.[32]

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

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

88. Defendant was at all times fully aware of its obligation to protect consumers' Private Information.[33] Defendant was also aware of the significant repercussions that would result from its failure to do so.

G. Defendant Failed to Comply with Industry Standards.

89. Experts studying cybersecurity routinely identify companies that come into possession of large amounts of Private Information, such as CommonSpirit, as being particularly vulnerable to cyberattacks because of the value of the information they maintain.

90. Several best practices have been identified that at a minimum should be implemented by healthcare providers like Defendant, including but not limited to: educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and antimalware software; encryption making data unreadable without a key; multi-factor authentication; backup data; and limiting which employees can access sensitive data.

91. Other best cybersecurity practices that are standard in the healthcare industry

---

[32] *See, e.g.*, *In the Matter of LabMd, Inc., A Corp.*, 2016-2 Trade Cas. (CCH) ¶ 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.").

[33] *See Notice of Privacy Practices*, Virginia Mason Franciscan Health, https://www.vmfh.org/content/dam/vmfhorg/pdf/vmfh-npp-english.pdf (last updated June 2022) (Defendant "understand[s] that [patent] protected health information is private and personal" and is "committed to protecting it").

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; and training staff regarding critical points.

92. 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 for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.[34]

93. These foregoing frameworks are existing and applicable industry standards in the healthcare industry, and Defendant failed to comply with these accepted standards, thereby opening the door to and causing the Data Breach and the resulting harm to Plaintiffs and the Class Members.

H. Defendant Failed to Comply with HIPAA

94. HIPAA requires covered entities like Defendant to protect against reasonably anticipated threats to the security of sensitive patient health information.

95. Covered entities (including Defendant) must implement safeguards to ensure the confidentiality, integrity, and availability of PHI. Safeguards must include physical, technical, and administrative components.

96. Title II of HIPAA contains what are known as the Administrative Simplification provisions. 42 U.S.C. §§ 1301, *et seq*. These provisions require, among other things, that the

[34] *See* https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf; https://www.nist.gov/cyberframework/getting-started; *see also* https://www.cisecurity.org/controls (last accessed Jan. 10, 2023).

Department of Health and Human Services ("HHS") create rules to streamline the standards for handling Private Information like the data Defendant left unguarded. The HHS subsequently promulgated multiple regulations under authority of the Administrative Simplification provisions of HIPAA. These rules include 45 C.F.R. § 164.306(a)(1-4); 45 C.F.R. § 164.312(a)(1); 45 C.F.R. § 164.308(a)(1)(i); 45 C.F.R. § 164.308(a)(1)(ii)(D); and 45 C.F.R. § 164.530(b).

97. 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.

98. Data breaches where an unauthorized individual gains access to PHI 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 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).[35]

99. Defendant's Data Breach resulted from a combination of insufficiencies that demonstrate Defendant failed to comply with safeguards and standards of care mandated by HIPAA regulations.

---

[35] *See also* Department of HHS Fact Sheet: Ransomware and HIPAA (July 11, 2016), available at https://www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf (last accessed Jan. 10, 2023).

I. CommonSpirit Knew of the Manifold Risks of Improperly Storing Valuable Private Information and Foreseeable Damages to Victims

100. The ramifications of Defendant's failure to keep the Private Information secure are long lasting and severe.

101. Once Private Information is stolen, fraudulent use of that information and damage to victims may continue for years as victims of data breaches are more likely to become victims of identity fraud.

102. The Private Information belonging to Plaintiffs and Class Members is personal, sensitive in nature and was left inadequately protected by Defendant who did not obtain Plaintiffs' or Class Members' consent to disclose such Private Information to any other person as required by applicable law and industry standards.

103. Identity thieves use stolen personal information for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud. Such fraud may go undetected for months, or even years.

104. 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.

105. Some consumers victimized by identity theft may lose out on job opportunities, or be denied loans for education, housing or cars because of negative information on their credit

reports. In rare cases, they may even be arrested for crimes they did not commit.

106. 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 identity fraud is only about 3%.[36]

107. Identity fraud of any kind can wreak havoc on a victim's life for years, but theft of PHI is especially damaging because criminals can destroy a victims' health insurance coverage and leave them without a safety net when they need it most.

108. Moreover, victims of medical identity theft could get bills for medical treatments never received.

109. In the digital age, bad data can cause a tangled mess that takes time to solve, but for people in need of urgent surgeries or treatment such delays can cause immense stress, not to mention seriously complicate the provision of needed medical treatments and services.

110. If a patient falls victim to medical identity theft, they also run the risk that Medicare and/or other health insurance benefits may be depleted when needed most.

111. Fraudulent treatments done under victims' names can completely change their medical information history, which could lead doctors to misdiagnose actual conditions or prescribe unnecessary treatments.

112. "About 20 percent of victims have told us that they got the wrong diagnosis or treatment, or that their care was delayed because there was confusion about what was true in their records due to the identity theft," says Ann Patterson, a senior vice president of the Medical

[36] 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 Jan. 13, 2023).

Identity Fraud Alliance (MIFA), a group of several dozen healthcare organizations and businesses working to reduce the crime and its negative effects.[37]

113. 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.

114. Sensitive Private Information can sell for as much as $363 per record, according to the Infosec Institute.[38] PHI is particularly valuable because criminals can use it to target victims with frauds and scams.

115. As with non-medical identity theft, dealing with the repercussions can be a confusing, time-consuming and costly process, but medical identity theft can also be more dangerous than other forms of identity fraud because it can lead to life-threatening errors in medical records and consequently treatments.[39]

116. The Data Breach was a direct and proximate result of Defendant's failure to: (i) properly safeguard and protect Plaintiffs' and Class Members' Private Information from unauthorized access, use, and disclosure as required by various state and federal regulations, industry practices and common law; (ii) establish and implement appropriate administrative, technical and physical safeguards to ensure the security and confidentiality of Plaintiffs' and Class Members' Private Information; and (iii) protect against reasonably foreseeable threats to the

---

37 *Id.*

38 *See* Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, InfoSec (July 27, 2015), available at https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/ (last accessed Jan. 10, 2023).

39 https://www.experian.com/blogs/ask-experian/how-prevent-medical-identity-theft/ (last accessed Jan. 10, 2023).

security or integrity of such information.

117. Had Defendant remedied the deficiencies in its data security systems and adopted security measures recommended by experts in the field, they would have prevented the intrusions into its systems.

118. As a direct and proximate result of Defendant's wrongful actions and inactions, Plaintiffs and Class Members have been placed at an imminent, immediate and continuing increased risk of harm from identity theft and fraud, requiring them to take the time which they otherwise would have dedicated to other life demands such as work and family in an effort to mitigate the actual and potential impact of the Data Breach on their lives.

119. The U.S. Department of Justice's Bureau of Justice Statistics found that "among victims who had Private information used for fraudulent purposes, 29% spent a month or more resolving problems" and that "resolving the problems caused by identity theft [could] take more than a year for some victims."[40]

120. The United States Government Accountability Office ("GAO") released a report in 2007 regarding data breaches 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."[41]

121. What's more, Private Information constitutes a valuable property right, the theft of which is gravely serious.[42] Its value is axiomatic, considering the value of Big Data in corporate

---

[40] U.S. Department of Justice, Office of Justice Programs Bureau of Justice Statistics, *Victims of Identity Theft, 2012* (Dec. 2013), available at https://bjs.ojp.gov/content/pub/pdf/vit12.pdf (last accessed Jan. 10, 2023).

[41] *See* "Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown," p.2, the GAO (June 2007), available at https://www.gao.gov/assets/gao-07-737.pdf (last accessed Jan. 10, 2023).

[42] *See, e.g.*, John T. Soma, et al, Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) ("PII, 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).

America, and the consequences of cyber thefts include heavy prison sentences. Even this obvious risk-to-reward analysis illustrates beyond doubt that Private Information has considerable market value.

122. It must also be noted there may be a substantial time lag—measured in years—between when harm occurs versus when it is discovered, and also between when PII and/or PHI information is stolen and when it is used.

123. According to the 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.[43]

124. PII and PHI are such valuable commodities to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black-market" for years.

125. Plaintiffs 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.

126. There is a strong probability that entire batches of stolen information have been dumped on the black market and are yet to be dumped on the black market, meaning Plaintiffs and Class Members are at an increased risk of fraud and identity theft for many years into the future. Thus, Plaintiffs and Class Members must vigilantly monitor their financial accounts for many years to come.

---

[43] *Id.*

REPRESENTATIVE PLAINTIFFS' EXPERIENCE

127. Plaintiffs Jose Antonio Koch and his minor children, John and James Doe, entrusted their Private Information to Defendant.

128. Specifically, Plaintiffs were patients at Defendant's St. Michael Medical Center in Silverdale, Washington.

129. As a condition of receiving medical products and services, Plaintiffs were required by Defendant to disclose their Private Information.

130. Plaintiffs provided their Private Information to CommonSpirit and trusted that the information would be safeguarded according to internal policies and state and federal law.

131. At the time of the Data Breach, Defendant retained Plaintiffs' name, address, diagnostic information, and health insurance information.

132. On December 1, 2022, Defendant notified Plaintiffs that its computer systems had been accessed and Plaintiffs' Private Information had been involved in the Data Breach.

133. Plaintiff Koch, on behalf of himself and the minor Plaintiffs, is very careful about sharing their sensitive PII and PHI. Plaintiff Koch, on behalf of himself and the minor Plaintiffs, has never knowingly transmitted unencrypted sensitive PII and PHI over the internet or any other unsecured source.

134. Plaintiff Koch, on behalf of himself and the minor Plaintiffs, stores any documents containing their sensitive PII and PHI in a safe and secure location or destroys the documents. Moreover, Plaintiff Koch, on behalf of himself and the minor Plaintiffs, diligently chooses unique usernames and passwords for their various online accounts.

135. As a result of the Data Breach notice, Plaintiff Koch, on behalf of himself and the minor Plaintiffs, spent time dealing with the consequences of the Data Breach, which includes time spent verifying the legitimacy of the Notice of Security Incident, self-monitoring their

accounts and credit reports to ensure no fraudulent activity has occurred.

136. This time has been lost forever and cannot be recaptured. Moreover, this time was spent at Defendant's direction by way of the Data Breach notice where Defendant advised Plaintiffs to mitigate their damages by, among other things, monitoring their health care accounts for accuracy.

137. Plaintiffs have suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from their PII and PHI being placed in the hands of unauthorized third parties and possibly criminals.

138. Plaintiffs have a continuing interest in ensuring that Plaintiffs' PII and PHI, which, upon information and belief, remain backed up in Defendant's possession, is protected, and safeguarded from future breaches.

PLAINTIFFS' & CLASS MEMBERS' DAMAGES

139. Plaintiffs and Class Members have suffered injury sufficient to confer standing under Article III of the United States Constitution.

140. Plaintiffs and Class Members have an "increased risk of identity theft or fraud following the unauthorized disclosure of their data." McMorris v. Lopez, 995 F.3d 295, 300-01 (2d Cir. 2021).

141. First, and most importantly, their Private Information has been compromised as the result of the Data Breach.

142. A third party intentionally targeted Defendant's computer system and stole Plaintiffs' Private Information stored on that system. *See* McMorris v. Lopez, 995 F.3d 295, 301 (2d Cir. 2021), quoting Remijas v. Neiman Marcus Grp., LLC, 794 F.3d 688, 693 (7th Cir. 2015) ("Why else would hackers break into a store's database and steal consumers' private information? Presumably, the purpose of the hack is, sooner or later, to make fraudulent charges or assume those

consumers' identities.").

143. The type of data at issue here will likely subject Plaintiffs and Class Members to a perpetual risk of medical or other identity theft or fraud.

144. The FTC recommends that identity theft 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 alert (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.[44]

145. To date, Defendant only blandly states that "it is always prudent for patients to review health care statements or accuracy, and report any services or charges that were not incurred to the provider or insurance carrier."[45]

146. Defendant's Notice to Plaintiffs does not even offer any credit monitoring services and/or other identity theft protection services.

147. The offer is wholly inadequate as it fails to provide for the fact that victims of data breaches and other unauthorized disclosures commonly face multiple years of ongoing identity theft, and it entirely fails to provide any compensation for the unauthorized release and disclosure of Plaintiffs' and Class Members' Private Information.

148. Furthermore, Defendant's Notice to Plaintiffs and Class Members squarely places the burden on Plaintiffs and Class Members, rather than on the Defendant, to investigate and protect themselves from Defendant's tortious acts resulting in the Data Breach.

149. Rather than automatically enrolling Plaintiffs and Class Members in credit monitoring services upon discovery of the Data Breach, Defendant, in a non-committal fashion,

---

[44] *See* IdentityTheft.gov by the Federal Trade Commission, https://www.identitytheft.gov/Steps (last accessed Jan. 10, 2023).

[45] *See* **Exhibit A**.

advises affected victims to "review […] additional steps [they] can take to protect [themselves or their child]," including placing "a fraud alert or security freeze" on their credit file.[46]

150. Plaintiffs and Class Members have been damaged by the compromise of their Private Information in the Data Breach.

151. Plaintiffs' PII and PHI were compromised as a direct and proximate result of the Data Breach.

152. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have been placed at an imminent, immediate, and continuing increased risk of harm from fraud and identity theft.

153. As a direct and proximate result of Defendant' conduct, Plaintiffs and Class Members have been forced to expend time dealing with the effects of the Data Breach.

154. Plaintiffs and Class Members face substantial risk of out-of-pocket fraud losses such as loans opened in their names, medical services billed in their names, tax return fraud, utility bills opened in their names, credit card fraud and similar identity theft.

155. Plaintiffs and Class Members face substantial risk of being targeted for future phishing, data intrusion and other illegal schemes based on their PII and PHI as potential fraudsters could use that information to more effectively target such schemes to Plaintiffs and Class Members.

156. Plaintiffs and Class Members may also incur out-of-pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees and similar costs directly or indirectly related to the Data Breach.

157. Plaintiffs and Class Members also suffered a loss of value of their Private

---

[46] *See* ***id.***

Information when it was acquired by cyber thieves in the Data Breach. Numerous courts have recognized the propriety of loss of value damages in related cases.

158. Plaintiffs and Class Members have spent and will continue to spend significant amounts of time to monitor their financial accounts and records for misuse.

159. Plaintiffs and Class Members have suffered or will suffer actual injury as a direct result of the Data Breach.

160. Moreover, Plaintiffs and Class Members have an interest in ensuring that their Private Information, which is believed to remain in the possession of Defendant, is protected from further breaches by the implementation of security measures and safeguards, including, but not limited to, making sure that the storage of data or documents containing personal, medical and financial information is not accessible online and that access to such data is password-protected.

161. As a direct and proximate result of Defendant's actions and inactions, Plaintiffs and Class Members have suffered anxiety, emotional distress and loss of privacy and are at an increased risk of future harm.

162. Moreover, Defendant's delay in identifying and reporting the Data Breach caused additional harm as it is self-evident that early notification can also help limit the liability of a victim in many cases.

163. Indeed, once a data breach has occurred, "[o]ne thing that does matter is hearing about a data breach quickly. That alerts consumers to keep a tight watch on credit card bills and suspicious emails. It can prompt them to change passwords and freeze credit reports. And notifying officials can help them catch cybercriminals and warn other businesses of emerging dangers. If consumers don't know about a breach because it wasn't reported, they can't take action to protect

themselves" (internal citations omitted).[47]

164. Although Defendant experienced a data breach which led to unauthorized exposure of patients' Private Information between September 16, 2022, and October 3, 2022, CommonSpirit did not issue any notice until starting in December of 2022, depriving Plaintiffs and Class Members of the ability to promptly mitigate potential adverse consequences resulting from the Data Breach.

165. As a result of Defendant's delay in detecting and notifying consumers of the Data Breach, the risk of fraud for Plaintiffs and Class Members needlessly increased.

ILLINOIS LAW SHOULD APPLY TO PLAINTIFFS AND THE CLASS AS WHOLE

166. The State of Illinois has a significant interest in regulating the conduct of businesses operating within its borders.

167. That is, Illinois, which seeks to protect the rights and interests of Illinois and all residents and citizens of the United States against a company headquartered and doing business in Illinois, has a greater interest in the claims of Plaintiffs and the Class than any other state and is most intimately concerned with the claims and outcome of this litigation.

168. The principal place of business and headquarters of Defendant, located in Illinois, is the "nerve center" of its business activities – the place where its high-level officers direct, control, and coordinate Defendant's and its affiliates' activities, including major policy, financial and legal decisions.

169. Defendant's actions and corporate decisions surrounding the allegations made herein were made from and in Illinois.

170. Defendant's breaches of duty to Plaintiffs and Class Members emanated from

[47] https://www.consumerreports.org/data-theft/the-data-breach-next-door-a7102554918/ (last accessed Jan. 10, 2023).

Illinois.

171. Application of Illinois law to the Class with respect to Plaintiffs' and the Class' claims is neither arbitrary nor fundamentally unfair because Illinois has significant contacts and a significant aggregation of contacts that create a state interest in the claims of Plaintiffs and the Class.

172. Under Illinois's choice of law principles, which are applicable to this action, the common law of Illinois applies to the nationwide common law claims of all Class members. In addition, given Illinois's significant interest in regulating the conduct of businesses operating within its borders, and that Illinois has the most significant relationship to Defendant, as it is headquartered in Illinois and its executives and officers are located and made decisions which led to the allegations of this litigation there, there is no conflict in applying Illinois law to non-resident consumers such as Plaintiffs and the Class.

CLASS ACTION ALLEGATIONS

173. Plaintiffs bring this action on behalf of himself and his minor children as well as on behalf of all other persons similarly situated.

174. Plaintiffs propose the following Class definition, subject to amendment as appropriate:

> All persons whose Private Information was compromised as a result of the Data Breach announced by Defendant on or about October 4, 2022 (the "Class").

175. Excluded from the Class are Defendant's officers and directors, and any entity in which Defendant has a controlling interest; and the affiliates, legal representatives, attorneys, successors, heirs, and assigns of Defendant. Excluded also from the Class are Members of the judiciary to whom this case is assigned, their families and Members of their staff.

176. Plaintiffs hereby reserve the right to amend or modify the class definitions with

greater specificity or division after having had an opportunity to conduct discovery and before the Court determines whether certification is appropriate. The proposed Class meets the criteria for certification under Rule 23(a), (b)(2), (b)(3) and (c)(4).

177. **Numerosity**. The Members of the Class are so numerous that joinder of all of them is impracticable. While the exact number of Class Members is unknown to Plaintiffs at this time, Defendant has identified more than 600 thousand persons whose Private Information may have been compromised in the Data Breach, and the victims are apparently identifiable within Defendant's records.

178. **Commonality and Predominance**. There are questions of law and fact common to the Class, which predominate over any questions affecting only individual Class Members. These include, without limitation:

a. Whether Defendant owed a duty to Class Members to safeguard their Private Information;

b. Whether Defendant unlawfully used, maintained, lost, or disclosed Plaintiffs' and Class Members' Private Information;

c. Whether Defendant breached its duty to Class Members to safeguard their Private Information;

d. Whether computer hackers obtained Class Members' Private Information in the Data Breach;

e. When specifically Defendant actually learned of the Data Breach;

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

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

h. Whether Defendant's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

i. Whether Defendant's data security systems prior to and during the Data Breach were consistent with industry standards;

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

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

l. Whether Plaintiffs and Class Members suffered legally cognizable damages as a result of Defendant's misconduct;

m. Whether Defendant's conduct was negligent;

n. Whether Defendant's conduct was *per se* negligent;

o. Whether Defendant was unjustly enriched; and

p. Whether Plaintiffs and Class Members are entitled to damages, civil penalties, punitive damages and/or injunctive relief.

179. Defendant engaged in a common course of conduct giving rise to the legal rights Plaintiffs and Class Members seek to enforce, in that all the Plaintiffs' and Class Members' data was stored on the same computer systems and unlawfully accessed in the same way. The common issues arising from Defendant's conduct affecting Class Members set out above predominate over any individualized issues. Similar or identical statutory and common law violations, business practices, and injuries are involved. Individual questions, if any, pale in comparison, in both quality and quantity, to the numerous common questions that dominate this action. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

180. **Typicality**. Plaintiffs' claims are typical of those of other Class Members because Plaintiffs' Private Information, like that of every other Class member, was compromised in the Data Breach.

181. **Adequacy of Representation.** Plaintiffs will fairly and adequately represent and protect the interests of the Members of the Class in that they have no disabling conflicts of interest

that would be antagonistic to that of the other Class Members. Plaintiffs seek no relief that is antagonistic or adverse to the Members of the Class and the infringement of the rights and the damages they have suffered are typical of other Class Members. Plaintiffs' Counsel is competent and experienced in litigating class actions, including data privacy litigation of this kind.

182. **Superiority**. A class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Defendant. In contrast, the conduct of this action as a class action presents far fewer management difficulties, conserves judicial resources and the parties' resources and protects the rights of each Class member.

183. 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.

184. 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.

185. Unless a Class-wide injunction is issued, Defendant may continue in its failure to properly secure the Private 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.

186. 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.

187. Finally, all members of the proposed Class are readily ascertainable and adequate notice can be given to Class Members directly using information maintained in Defendant's records.

CAUSES OF ACTION

Count I

NEGLIGENCE
(On Behalf of Plaintiffs & All Class Members)

188. Plaintiffs reallege and incorporate by reference the preceding paragraphs as if fully set forth herein.

189. Defendant obtained Plaintiffs' and Class Members' Private Information as a condition of providing services to Plaintiffs and Class Members.

190. Defendant's acceptance and maintenance of this information is for its own pecuniary gain and as part of its regular business activities.

191. Plaintiffs and the Class Members entrusted their Private Information to Defendant on the premise and with the understanding that Defendant would safeguard their information, use their Private Information for business purposes only, and/or not disclose their Private Information to unauthorized third parties.

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

193. Defendant knew or reasonably should have known that the failure to exercise due care in the collecting, storing, and using of their consumers' Private Information involved an unreasonable risk of harm to Plaintiffs and Class Members, even if the harm occurred through the criminal acts of a third party.

194. 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.

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

196. 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.

197. 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.

198. By assuming the responsibility to collect and to 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 its computer property—and Class Members' Private Information held within it— to prevent disclosure of the information, and to safeguard the information from theft. Defendant's duty included a responsibility to implement security protocols and processes by which it could detect a breach of its network servers in a reasonably expeditious period of time and give prompt notice to those affected in the case of a data breach.

199. 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.

200. 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 Private Information.

201. Defendant breached its duties (and thus was negligent) by failing to use reasonable measures to protect Class Members' Private Information. The specific negligent acts and omissions committed by Defendant includes, but are not limited to, the following:

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

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

c. Failing to periodically ensure that its computer system had plans in place to maintain reasonable data security safeguards;

d. Failing to meet the minimum industry standards for preventing cyberattacks and data breaches;

e. Improperly and inadequately safeguarding the Private Information of Plaintiffs and Class Members in deviation of standard industry rules, regulations, and practices at the time of the Data Breach;

f. Failing to heed industry warnings and alerts to provide adequate safeguards to protect consumers' Private Information in the face of increased risk of theft;

g. Allowing unauthorized access to Class Members' Private Information;

h. Failing to detect in a timely manner that Class Members' Private Information had been compromised; and

i. Failing to timely and adequately notify Class Members about the existence and scope of the Data Breach so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

202. It was foreseeable that Defendant's failure to use reasonable measures to protect Class Members' Private Information would result in injury to Class Members.

203. Further, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches.

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

205. Plaintiffs and Class Members had no ability to protect their Private Information that was in, and possibly remains in, Defendant's possession.

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

207. Defendant had and continues to have a duty to adequately and promptly disclose that the Private Information of Plaintiffs and Class Members 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 Class Members to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their Private

Information by third parties.

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

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

210. There is a temporal and close causal connection between Defendant's failure to implement security measures to protect the Private Information and the harm suffered, or risk of imminent harm suffered by Plaintiffs and Class Members.

211. As a result of Defendant's negligence, Plaintiffs and Class Members have suffered and will continue to suffer damages and injury including, but not limited to: out-of-pocket expenses associated with procuring robust identity protection and restoration services; increased risk of future identity theft and fraud, the costs associated therewith; time spent monitoring, addressing and correcting the current and future consequences of the Data Breach; and the necessity to engage legal counsel and incur attorneys' fees, costs and expenses.

212. Additionally, as a direct and proximate result of Defendant's negligence Plaintiffs and Class members have suffered and will suffer the continued risks of exposure of their Private Information, which remains 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 Private Information in its continued possession.

213. Plaintiffs and Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach. 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 and continue to provide adequate credit monitoring to all Class Members.

Count II

BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiffs & All Class Members)

214. Plaintiffs reallege and incorporate by reference the preceding paragraphs as if fully set forth herein.

215. Plaintiffs and Class Members were required to provide their Private Information to Defendant as a condition of their use of Defendant's services.

216. Plaintiffs and Class Members paid money to Defendant in exchange for services, along with Defendant's promise to protect their Private Information from unauthorized access and disclosure.

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

218. When Plaintiffs and Class Members provided their PII and PHI to Defendant, they entered into implied contracts with Defendant pursuant to which Defendant agreed to reasonably protect such information.

219. 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.

220. Plaintiffs and Class Members would not have entrusted their Private Information to Defendant in the absence of the implied contract between them and Defendant to keep their information reasonably secure, including monitoring its computer systems and networks to ensure that it adopted reasonable data security measures.

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

222. Defendant breached its implied contracts with Class Members by failing to safeguard and protect their Private Information.

223. As a direct and proximate result of Defendant's breaches of the implied contracts, Class Members sustained damages as alleged herein.

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

225. 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 and continue to provide adequate credit monitoring to all Class Members.

COUNT III

UNJUST ENRICHMENT
(On Behalf of Plaintiffs & All Class Members)

226. Plaintiffs reallege and incorporate by reference the preceding paragraphs as if fully set forth herein.

227. Upon information and belief, Defendant funds its data security measures from its

general revenue including payments made by or on behalf of Plaintiffs and the Class Members.

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

229. Plaintiffs and Class Members conferred a monetary benefit on Defendant.

230. Specifically, they purchased goods and services from Defendant and in so doing provided Defendant with their Private Information. In exchange, Plaintiffs and Class Members should have received from Defendant the goods and services that were the subject of the transaction and have their Private Information protected with adequate data security.

231. Defendant was aware that any payment for its services was intended for it on behalf of the consumer as each individual for which Defendant maintained private information was identifiable via the information Defendant collected.

232. Defendant knew that Plaintiffs and Class Members conferred a benefit which Defendant accepted. Defendant profited from these transactions and used the Private Information of Plaintiffs and Class Members for business purposes.

233. In particular, Defendant enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiffs' and Class Members' Private Information. Instead of providing a reasonable level of security that would have prevented the Data Breach, Defendant instead calculated to increase its own profits at the expense of Plaintiffs and Class Members by utilizing cheaper, ineffective security measures. 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.

234. Under the principles of equity and good conscience, Defendant should not be permitted to retain the money belonging to Plaintiffs and Class Members because Defendant failed

to implement appropriate data management and security measures that are mandated by industry standards.

235. Defendant failed to secure Plaintiffs and Class Members' Private Information and, therefore, did not provide full compensation for the benefit Plaintiffs and Class Members provided.

236. Defendant acquired the Private Information through inequitable means in that it failed to disclose the inadequate security practices previously alleged.

237. If Plaintiffs and Class Members knew that Defendant had not secured their Private Information, they would not have agreed to provide their Private Information to Defendant.

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

239. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity how their Private Information is used; (iii) the compromise, publication and/or theft of their Private Information; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their Private Information; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (vi) the continued risk to their Private Information, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect PII and PHI in its continued possession; and (vii) future costs in terms of time, effort and money that will be expended to prevent, detect, contest and repair the impact of the Private Information compromised as a result of the Data Breach, for the remainder of the lives of Plaintiffs and Class Members.

240. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class

Members have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and noneconomic losses.

241. Defendant should be compelled to disgorge into a common fund or constructive trust for the benefit of Plaintiffs and Class Members the proceeds that it unjustly received from them.

COUNT IV

NEGLIGENCE *PER SE*
(On Behalf of Plaintiffs & All Class Members)

242. Plaintiffs reallege and incorporate by reference the preceding paragraphs as if fully set forth herein.

243. Defendant's duty of care to use reasonable security measures also arose as a result of the special relationship that existed between Defendant and its patients, which is recognized by laws and regulations including but not limited to HIPAA, as well as common law. Defendant was in a position to ensure that its systems were sufficient to protect against the foreseeable risk of harm to Class Members from a Data Breach or data breach.

244. 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, dental, and/or medical information at issue in this case constitutes "protected health information" within the meaning of HIPAA.

245. Defendant's violation of 45 C.F.R. § 164.530(c)(l) and related HIPAA provisions constitutes negligence *per se*.

246. Pursuant to the Federal Trade Commission Act (15 U.S.C. § 45), Defendant had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiffs' and Class Members' Private Information.

247. Additionally, 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 businesses, such as Defendant, of failing to use reasonable measures to protect Private Information. The FTC publications and orders described above also form part of the basis of Defendant's duty in this regard.

248. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect Plaintiffs' and Class Members' Private Information and not complying with applicable industry standards, as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of Private Information it obtained and stored and the foreseeable consequences of a data breach including, specifically, the damages that would result to Plaintiffs and Class Members.

249. Defendant's violation of Section 5 of the FTC Act constitutes negligence *per se* as Defendant's violation of the FTC Act establishes the duty and breach elements of negligence.

250. Plaintiffs and Class Members are within the class of persons that the FTC Act was intended to protect.

251. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses which—as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices—caused the same harm as that suffered by Plaintiffs and Class Members.

252. But for Defendant's wrongful and negligent breach of its duties owed to Plaintiffs and Class Members, Plaintiffs and Class Members would not have been injured.

253. Defendant knew or should have known that it was failing to meet its duties and that its breach would cause Plaintiffs and Class Members to experience the foreseeable harms associated with the exposure of their Private Information.

254. As a direct and proximate result of Defendant's negligent conduct, Plaintiffs and Class Members have suffered and will continue to suffer injury and damages as alleged herein, and are entitled to compensatory, consequential and punitive damages in an amount to be proven at trial.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs Jose Antonio Koch, on behalf of minors John and James Doe, and on behalf of all others similarly situated respectfully 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;

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' Private 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 Private Information compromised during the Data Breach;

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

e) Ordering Defendant to pay for not less than seven years of credit monitoring services for Plaintiffs and Class Members;

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

g) For an award of punitive damages as allowable by law;

h) For an award of attorneys' fees and costs and any other expense, including expert witness fees;

i) Pre- and post-judgment interest on any amounts awarded; and

j) Such other and further relief as this Honorable Court may deem just and proper.

JURY TRIAL DEMANDED

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

Dated: January 13, 2023

Respectfully submitted,

KHOWAJA LAW FIRM, LLC

s/ Kasif Khowaja .

Kasif Khowaja
Paul Castiglione
Khowaja Law Firm, LLC
8 South Michigan Ave, Suite 2600
Chicago, IL 60603
(312) 566-8070
kasif@khowajalaw.com
pcastig@khowajalaw.com

Counsel for Plaintiffs and the Nationwide Class

Exhibit A

CommonSpirit

December 1, 2022

16 1 5783 ********AUTO**5-DIGIT 98013
Parents of

BAINBRIDGE IS, WA 98110-1823

Dear Parents of ,

CommonSpirit Health and its affiliated entities ("CommonSpirit") take the protection and proper use of your or your child's personal information very seriously. With that in mind, we are writing to tell you about a data security incident involving some of your or your child's personal information. While we have no evidence of misuse of your or your child's personal information, we are writing to you directly to explain the incident, our response to it, and steps you can take in addition to those you take every day to protect your or your child's personal information, should you feel it appropriate to do so.

What happened?

On October 2, 2022, CommonSpirit detected activity on our IT network that we later determined was ransomware. We immediately took steps to secure the network, which included proactively taking certain systems offline, and began an investigation with the assistance of an external leading cybersecurity specialist. The investigation determined that an unauthorized third party gained access to certain portions of our network between September 16, 2022 and October 3, 2022. During that time, the unauthorized third party may have gained access to certain files, including files that contained personal information. While the review of these files is ongoing, we identified that some of this data was associated with services provided in the past by Franciscan Medical Groups and/or Franciscan Health in Washington State. Franciscan Health includes St. Michael Medical Center (formerly Harrison Hospital), St. Anne Hospital (formerly Highline Hospital), St. Anthony Hospital, St. Clare Hospital, St. Elizabeth Hospital, St. Francis Hospital, and St. Joseph Hospital. Those facilities are now known collectively as Virginia Mason Franciscan Health, which is an affiliated entity of CommonSpirit.

What information was involved?

Our information shows that you or your child may have been a patient at one of the impacted facilities. You are being notified because some of your or your child's information was identified in the compromised files.

While the review of the files is ongoing, we identified that the information in some of the files included your or your child's name, address, date of birth, phone number(s), and a unique ID number used only internally within our organization.

What we are doing.

Upon discovering the ransomware attack, CommonSpirit quickly mobilized to protect its systems, contain the incident, begin an investigation, and maintain continuity of care. In addition, CommonSpirit notified law enforcement and is supporting their ongoing investigation. Once secured, systems were returned to the network with additional security and monitoring tools.

Actions you may wish to take.

Though CommonSpirit has no evidence that any personal information has been misused as a result of the incident, it is always prudent for patients to review health care statements for accuracy, and report any services or charges that were not incurred to the provider or insurance carrier. Additionally, please review the enclosed "Additional Resources" section of this letter. That section describes additional steps you can take to help protect yourself or your child, including recommendations by the Federal Trade Commission regarding identity theft protection and details on how to place a fraud alert or a security freeze on your credit file if you desire to do so.

ELN-16342-5783

For more information.

If you need more information about this event, we established a special call center through our third party partner Kroll that can answer specific questions about this event. To contact this special call center, please call (855) 504-2738, Monday through Friday from 7:00 a.m. to 4:30 p.m. Pacific Time, excluding U.S. holidays.

We apologize for any concern this may cause. Protecting your information is important to us. We trust that this notification and additional resource information demonstrates our continued commitment to you.

Sincerely,

Lori Lamb

Lori Lamb
National Privacy Officer
CommonSpirit Health