IN THE UNITED STATES DISTRICT COURT
FOR THE MIDDLE DISTRICT OF TENNESSEE
NASHVILLE DIVISION

---

TIMOTHY FERGUSON, on behalf of himself and all others similarly situated,

Plaintiff,

v.

Case No.: _____
JURY DEMANDED

COMMUNITY HEALTH SYSTEMS, INC. and CHSPSC, LLC,

Defendants.

---

**CLASS ACTION COMPLAINT**

---

Plaintiff Timothy Ferguson ("Plaintiff") brings this Class Action Complaint on behalf of himself, and all others similarly situated, against Defendants Community Health Systems, Inc. ("CHS") and CHSPSC, LLC ("CHSPSC," and collectively with CHS, "Defendants"), alleging as follows based upon information and belief and investigation of counsel, except as to the allegations specifically pertaining to him, which are based on personal knowledge:

## NATURE OF THE ACTION

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

2. The harm resulting from a data and privacy breach manifests in a number of ways, including identity theft and financial fraud, and the exposure of a person's PII or PHI through a

data breach ensures that such person will be at a substantially increased and certainly impending risk of identity theft crimes compared to the rest of the population, potentially for the rest of their lives. Mitigating that risk—to the extent it is even possible to do so—requires individuals to devote significant time and money to closely monitor their credit, financial accounts, health records, and email accounts, and take a number of additional prophylactic measures.

3. Defendant CHS is one of the nation's largest healthcare providers, operating 78 hospitals and more than 1,000 other care sites across 15 states. Defendant CHSPSC is a professional services company that provides services to hospitals and clinics affiliated with CHS.[1]

4. As a healthcare provider, Defendants knowingly obtain sensitive patient PII and PHI and have a resulting duty to securely maintain such information in confidence.

5. On February 13, 2023, Defendants disclosed to the Securities and Exchange Commission that their secure file transfer platform was accessed by unauthorized parties, compromising the patient PII and PHI stored therein (the "Data Breach").[2]

6. The notorious Clop ransomware gang took responsibility for the Data Breach.[3]

7. Based on the public statements of Defendants to date, a wide variety of PII and PHI was implicated in the Data Breach, including but not limited to an individual's full name, address,

---

[1] *See Community Health Systems*, https://www.chs.net/ (last visited Apr. 25, 2023); https://www.chs.net/; *Notice of Third-Party Security Incident Impacting CHSPSC Affiliate Data*, Community Health Systems, https://www.chs.net/notice-of-third-party-security-incident-impacting-chspsc-affiliate-data/ (last visited Apr. 25, 2023) ("*Notice of Data Breach*");

[2] Dissent, *Community Health Systems Estimates 1 million patients impacted by vendor's GoAnywhere breach*, DataBreaches.net (Feb. 13, 2023), https://www.databreaches.net/community-health-systems-estimates-1-million-patients-impacted-by-vendors-goanywhere-breach/.

[3] Sergiu Gatlan, *Healthcare giant CHS reports first data breach in GoAnywhere hack*, BleepingComputer (Feb. 14, 2023), https://www.bleepingcomputer.com/news/security/healthcare-giant-chs-reports-first-data-breach-in-goanywhere-hacks/.

medical billing and insurance information, certain medical information such as diagnoses and medication, and demographic information such as date of birth and Social Security number.[4]

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

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

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

## PARTIES

11. Plaintiff Timothy Ferguson is an adult, who at all relevant times, is a resident and citizen of the Commonwealth of Pennsylvania. Plaintiff was a patient at one of Defendants' hospitals in Pennsylvania. Plaintiff received a Data Breach notice from Defendants informing him that his PII and PHI that he entrusted to Defendants was compromised in the Data Breach.

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

[4] *Notice of Data Breach, supra* note 1.

13. Defendant CHS is a Delaware corporation with a principal place of business located at 4000 Meridian Blvd., Franklin, Tennessee 37067. Defendant CHS is the ultimate parent company of Defendant CHSPSC.

14. Defendant CHSPSC is a Delaware limited liability company with a principal place of business located at 4000 Meridian Blvd., Franklin, Tennessee 37067. Defendant CHSPSC is a single member limited liability company, and upon information and belief, that sole member is Defendant CHS. Defendant CHSPSC is a citizen of each state in which one of its members is a citizen. As such, Defendant CHSPSC is a citizen of the State of Tennessee.

## JURISDICTION AND VENUE

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

16. This Court has personal jurisdiction over Defendants because they reside in this District, and at all relevant times, engaged in substantial business activities in Tennessee.

17. Venue is proper in this District pursuant to 28 U.S.C. § 1391(b)(1) and (2), because Defendants reside in this District, and a substantial part of the acts, omissions, and events giving rise to the claims occurred in this District.

## FACTUAL BACKGROUND

### A. Defendants and the Services They Provide.

18. Defendants tout themselves as one of the nation's largest providers of healthcare services, operating hospitals and other care facilities across fifteen states.

19. Upon information and belief, while Defendants administer healthcare services, Defendants receive, maintain, and handle PII and PHI from their patients, which includes, inter-alia, full name, address, medical billing and insurance information, certain medical information such as diagnoses and medication, and demographic information such as date of birth and Social Security number.

20. Plaintiff and Class Members directly or indirectly entrusted Defendants with their sensitive and confidential PII and PHI and therefore reasonably expected that Defendants would safeguard their highly sensitive information and keep their PHI confidential.

21. As a custodian of Plaintiff's and Class Members' PII and PHI, Defendants assumed equitable and legal duties to safeguard and keep confidential Plaintiff's and Class Members' highly sensitive information, to only use this information for business purposes, and to only make authorized disclosures.

22. Despite Defendants stating that they "are committed to protecting [patients'] personal information," Defendants nevertheless failed to secure the PII and PHI of the individuals that provided them with sensitive information, resulting in the Data Breach and compromise of Plaintiff's and Class Members' PII and PHI.[5]

23. Defendants' data security obligations were particularly important given the substantial increase in cyber-attacks and/or data breaches preceding the date it disclosed the Data Breach.

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

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

[5] *Notice of Data Breach*, *supra* note 1.

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

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

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

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

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

---

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

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

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

30. The healthcare industry has become a prime target for threat actors: "High demand for patient information and often-outdated systems are among the nine reasons healthcare is now the biggest target for online attacks."[9] This is in part because now more than ever, healthcare companies "are using electronic records and tapping digital services" "creating more opportunities for cybercriminals."

31. Additionally, "[h]ospitals store an incredible amount of patient data. Confidential data that's worth a lot of money to hackers who can sell it easily – making the industry a growing target."[10]

32. Indeed, cybercriminals seek out PHI at a greater rate than other sources of personal information. Between 2009 and 2022, 5,150 healthcare data breaches of 500 or more individuals have been reported to Health and Human Services' Office of Civil Rights, resulting in the exposure or unauthorized disclosure of the information of 382,262,109 individuals—"[t]hat equates to more than 1.2x the population of the United States."[11]

33. Further, the rate of healthcare data breaches has been on the rise in recent years. "In 2018, healthcare data breaches of 500 or more records were being reported at a rate of around 1 per day. Fast forward 5 years and the rate has more than doubled. In 2022, an average of 1.94 healthcare data breaches of 500 or more records were reported each day."[12]

34. In a 2022 report, the healthcare compliance company Protenus found that there were 905 medical data breaches in 2021, leaving over 50 million patient records exposed for 700

---

Apr. 25, 2023).

[9] *The healthcare industry is at risk*, SwivelSecure https://swivelsecure.com/solutions/healthcare/healthcare-is-the-biggest-target-for-cyberattacks/ (last visited Apr. 25, 2023).

[10] *Id.*

[11] *Healthcare Data Breach Statistics*, HIPAA Journal, https://www.hipaajournal.com/healthcare-data-breach-statistics/ (last visited Apr. 24, 2023).

[12] *Id.*

of the 2021 incidents. This is an increase from the 758 medical data breaches that Protenus compiled in 2020.[13]

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

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

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

---

[13] *2022 Breach Barometer*, PROTENUS, https://www.protenus.com/breach-barometer-report (last visited Apr. 25, 2023).

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

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

[16] *Managing cyber risks in an interconnected world, Key findings from The Global State of Information Security® Survey 2015*, PriceWaterhouseCoopers, https://www.pwc.com/gx/en/consulting-services/information-security-survey/assets/the-global-state-of-information-security-survey-2015.pdf (last visited Apr. 25, 2023).

38. According to Experian:

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

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

40. 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

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

[18] U.S. Gov't Accountability Office, Report to Congressional Requesters, Personal Information, June 2007: https://www.gao.gov/new.items/d07737.pdf (last visited Apr. 25, 2023).

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.

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

**C. Defendants Show a Reckless Disregard for Data Security.**

42. As one of the largest healthcare providers in the United States, Defendants have an obligation to securely maintain the PII and PHI to which they are entrusted and keep it safe from harm. Defendants know that the PII and PHI they collect and maintain are prime targets for cybercriminals. Yet, Defendants have major security problems that pose a threat to their patients' sensitive information.

43. The current Data Breach is not the first time that Defendants have failed to protect their patients' PII and PHI from actors with nefarious intentions. In 2014, Defendants suffered a data breach during which hackers installed malware on Defendants' computer systems, compromising the PHI of 6.1 million individuals.[19] The information compromised during the 2014 data breach included names, phone numbers, addresses, dates of birth, sex, ethnicity, Social Security numbers, and emergency contact information.[20]

44. As a result of the 2014 data breach, Defendants were investigated by Health and Human Services' Office of Civil Rights ("OCR"). An audit completed by OCR revealed that Defendants had failed to implement security protections as required by the Health Insurance

[19] *Community Health Systems Pay $5 Million to Settle Multi-State Breach Investigation*, HIPAA Journal (Oct. 9, 2020), https://www.hipaajournal.com/community-health-systems-pays-5-million-to-settle-multi-state-breach-investigation/.
[20] *Id.*

Portability and Accountability Act ("HIPAA"), 42 U.S.C. § 1302d, *et seq*.[21] Indeed, according to the agency, "OCR's investigation found longstanding, systemic noncompliance with the HIPAA Security Rule including failure to conduct a risk analysis, and failures to implement information system activity review, security incident procedures, and access controls."[22]

45. To resolve Defendants' potential violations of HIPAA, in 2020 Defendants agreed to pay $2.3 million dollars to OCR and implement and maintain new cybersecurity measures to safeguard PHI.[23]

46. Despite Defendants' "new" cybersecurity plan, Defendants nevertheless suffered a second data breach less than three years later, again compromising patients' sensitive information.

**D. Defendants Breached Their Duty to Protect PII and PHI.**

47. Defendants engaged Fortra LLC ("Fortra") to provide them with a secure file transfer software—GoAnywhere MFT. "The GoAnywhere MFT is a web-based and managed file transfer tool designed to help organizations transfer files securely with partners and keep audit logs of who accessed the shared files."[24]

48. However, the GoAnywhere MFT software contained a major security vulnerability that could be exploited by criminal actors who wished to steal sensitive data contained on the file transfer platform.

---

[21] Hannah Ruhoff, *Mississippi Health-Care System Reports Data Breach*, Government Technology (Mar. 9, 2023), https://www.govtech.com/security/mississippi-health-care-system-reports-data-breach.

[22] Kat Jercich, *OCR levies $2.3M fine over massive breach affecting PHI of 6M people*, Healthcare News (Spt. 24, 2020), https://www.healthcareitnews.com/news/ocr-levies-23m-fine-over-massive-breach-affecting-phi-6m-people.

[23] *Id.*

[24] Sergiu Gatlan, *Exploit released for actively exploited GoAnywhere MFT zero-day*, BleepingComputer (Feb. 6, 2023), https://www.bleepingcomputer.com/news/security/exploit-released-for-actively-exploited-goanywhere-mft-zero-day/.

49. In mid-February 2023, Defendants announced that they had been impacted by a security incident involving the GoAnywhere MFT software.[25]

50. According to Defendants, between January 28 and January 30, 2023, Fortra discovered that unauthorized parties gained access to the GoAnywhere MFT software, compromising sets of files throughout the file transfer platform.[26]

51. On or about February 2, 2023, Defendants were then notified of the Data Breach and initiated their own investigation to determine the extent to which patient information was impacted.[27]

52. Defendants' investigation confirmed that wide swaths of sensitive information were exposed during the Data Breach including an individual's full name, address, medical billing and insurance information, certain medical information such as diagnoses and medication, and demographic information such as date of birth and social security number.[28]

53. The notorious Clop ransomware gang has since claimed responsibility for the Data Breach, informing BleepingComputer that Clop breached and stole data from over 130 organizations who utilized the GoAnywhere MFT software.[29] Clop was able to breach GoAnywhere MFT software by successfully exploiting a zero-day vulnerability which allowed the hackers to create unauthorized user accounts and leverage those user accounts to download files contained in the file share platform.[30]

---

[25] *Community Health Systems to Notify Up to 1 Million Individuals About GoAnywhere Data Breach*, HIPAA Journal (Mar. 10, 2023), https://www.hipaajournal.com/community-health-systems-goanywhere-data-breach/.
[26] *Notice of Data Breach*, *supra* note 1.
[27] *Id.*
[28] *Notice of Data Breach*, *supra* note 1.
[29] Gatlan, *supra* note 3.
[30] Ravie Lakshmanan, *Fortra Shed light on GoAnywhere MF Zero-Day Exploit used in Ransomware Attacks*, The Hacker News (Apr. 20, 2023),

54. On or about March 16, 2023, Defendants reported the Data Breach to OCR, indicating that approximately 962,000 individuals were impacted by the Data Breach.[31]

55. Despite discovering the Data Breach in early February, Defendants waited over a month to begin informing impacted patients. Indeed, Plaintiff did not receive a data breach notice informing him that his PII and PHI had been compromised during the Data Breach until on or about March 24, 2023.

56. Upon information and belief, Class Members received similar Data Breach notices on or around March 24, 2023, informing them that their PII and/or PHI was exposed during the Data Breach.

57. On or about April 17, 2023, Defendants issued supplemental notice to the Office of the Maine Attorney General, indicating the Data Breach was larger than initially reported and actually impacted approximately 1,173,000 individuals.[32]

58. The Data Breach occurred as a direct result of Defendants' failure to implement and follow basic data security procedures in order to protect individuals' PII and PHI. Defendants could have prevented the Data Breach, or substantially mitigated its severity, if they properly screened their vendors or contractors, such as Fortra, for cybersecurity standards as well as conducting cybersecurity audits of their contractors and vendors.

**E. Defendants Are Obligated Under HIPAA to Safeguard Personal Information.**

59. Defendants are required by the HIPAA to safeguard patient PHI.

---

https://thehackernews.com/2023/04/fortra-sheds-light-on-goanywhere-mft.html.

[31] *Breach Portal*, U.S. Dep't of Health & Human Services Office for Civil Rights, https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf, (last visited Apr. 25, 2023).

[32] *Data Breach Notifications*, Office of the Maine Attorney General (Apr. 17, 2023), https://apps.web.maine.gov/online/aeviewer/ME/40/810b151b-febe-43ef-9b77-b4c8ea0d9f4d.shtml.

60. Defendants are entities covered by HIPAA, which sets minimum federal standards for privacy and security of PHI.

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

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

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

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

65. The HIPAA Breach Notification Rule, 45 C.F.R. §§ 164.400-414, also requires Defendants to provide notice of the Data Breach to each affected individual "without unreasonable delay and in no case later than 60 days following discovery of the breach."[33]

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

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

68. Given the application of HIPAA to Defendants, and that Plaintiff and Class Members directly or indirectly entrusted their PHI to Defendants in order to receive healthcare services from Defendants, Plaintiff and Class Members reasonably expected that Defendants would safeguard their highly sensitive information and keep their PHI confidential.

## F. FTC Guidelines Prohibit Defendants from Engaging in Unfair or Deceptive Acts or Practices.

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

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

70. The FTC has promulgated numerous guides for businesses that highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[34]

71. The FTC provided cybersecurity guidelines for businesses, advising that businesses should protect personal customer information, properly dispose of personal information that is no longer needed, encrypt information stored on networks, understand their network's vulnerabilities, and implement policies to correct any security problems.[35]

72. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to private data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.[36]

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

74. Defendants were at all times fully aware of its obligations to protect the PII and PHI of patients because of its position as a healthcare provider, which gave them direct access to

[34] *Start with Security – A Guide for Business*, United States Federal Trade Comm'n (2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf.
[35] *Protecting Personal Information: A Guide for Business*, United States Federal Trade Comm'n, https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.
[36] *Id.*

reams of patient PII and PHI. Defendants were also aware of the significant repercussions that would result from its failure to do so.

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

**G. Plaintiff and Class Members Have Suffered Damages.**

76. As a result of Defendants' failure to implement and follow even the most basic security procedures, Plaintiff's and Class Members' PII/PHI has been and is now in the hands of unauthorized individuals, which may include thieves, unknown criminals, banks, credit companies, and other potentially hostile individuals and entities. Plaintiff and other Class Members now face an increased risk of identity theft, and will consequentially have to spend, and will continue to spend, significant time and money to protect themselves due to the Data Breach.

77. Plaintiff and other Class Members have had their most sensitive PII/PHI disseminated to the public at large and have experienced and will continue to experience emotional pain and mental anguish and embarrassment.

78. Plaintiff and Class Members face an increased risk of identity theft, phishing attacks, and related cybercrimes because of the Data Breach. Those impacted are under heightened and prolonged anxiety and fear, as they will be at risk of falling victim to cybercrimes for years to come.

79. PII/PHI is a valuable property right.[37] "Firms are now able to attain significant

[37] *See* Marc van Lieshout, *The Value of Personal Data* at p. 4, 457 IFIP ADVANCES IN INFORMATION AND COMMUNICATION TECHNOLOGY 26 (May 10, 2015), https://www.researchgate.net/publication/283668023_The_Value_of_Personal_Data ("The value of [personal] information is well understood by marketers who try to collect as much data about

market valuations by employing business models predicated on the successful use of personal data within the existing legal and regulatory frameworks."[9] American companies are estimated to have spent over $19 billion acquiring personal data of consumers in 2018.[10] It is so valuable to identity thieves that once PII/PHI has been disclosed, criminals often trade it on the "cyber black-market," or the "dark web," for many years.

80. As a result of its real value and the recent large-scale data breaches, identity thieves and cybercriminals have openly posted credit card numbers, Social Security numbers, PII/PHI, and other sensitive information directly on various Internet websites, making the information publicly available. This information from various breaches, including the information exposed in the Data Breach, can be aggregated and become more valuable to thieves and more damaging to victims, including Plaintiff and Class Members.

81. Personal information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[11] Experian reports that a stolen credit or debit card number can sell for $5 to $110 on the dark web.[12] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[13]

82. PHI is particularly valuable. All-inclusive health insurance dossiers containing sensitive health insurance information, names, addresses, telephone numbers, email addresses, Social Security numbers and bank account information, complete with account and routing numbers, can fetch up to $1,200 to $1,300 each on the black market.[38] According to a report released by the Federal Bureau of Investigation's ("FBI") Cyber Division, criminals can sell

---

personal conducts and preferences as possible[.]") (last visited Apr. 25, 2023).

[38] Adam Greenberg, *Health Insurance Credentials Fetch High Prices in the Online Black Market*, SC Magazine (July 16, 2013), https://www.scmagazine.com/home/security-news/health-insurance-credentials-fetch-high-prices-in-the-online-black-market/.

healthcare records for 50 times the price of a stolen Social Security or credit card number.[39]

83. Recognizing the high value that consumers place on their PII/PHI, some companies now offer consumers an opportunity to sell this information to advertisers and other third parties. The idea is to give consumers more power and control over the type of information they share and who ultimately receives that information. By making the transaction transparent, consumers will make a profit from the surrender of their PII/PHI.[40] This business has created a new market for the sale and purchase of this valuable data.[41]

84. Consumers place a high value on the privacy of that data. Researchers shed light on how much consumers value their data privacy—and the amount is considerable. Indeed, studies confirm that "when privacy information is made more salient and accessible, some consumers are willing to pay a premium to purchase from privacy protective websites."[42]

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

86. Cyberattacks have become so notorious that the FBI and U.S. Secret Service have issued a warning to potential targets, so they are aware of and prepared for a potential attack. As one report explained, "[e]ntities like smaller municipalities and hospitals are attractive to

---

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

[40] Steve Lohr, *You Want My Personal Data? Reward Me for It*, N.Y. Times (July 16, 2010), https://www.nytimes.com/2010/07/18/business/18unboxed.html.

[41] *See* Julia Angwin and Emil Steel, *Web's Hot New Commodity: Privacy*, WSJ (Feb. 28, 2011), https://www.wsj.com/articles/SB10001424052748703529004576 160764037920274.

[42] Janice Y. Tsai, *et al.*, *The Effect of Online Privacy Information on Purchasing Behavior, An Experimental Study*, 22(2) INFORMATION SYSTEMS RESEARCH 254 (June 2011), https://www.jstor.org/stable/23015560?seq=1 (last visited March 1, 2023).

ransomware criminals . . . because they often have lesser IT defenses and a high incentive to regain access to their data quickly.[43]

87. Plaintiff and members of the Class, as a whole, must immediately devote time, energy, and money to: (1) closely monitor their bills, records, and credit and financial accounts; (2) change login and password information on any sensitive account even more frequently than they already do; (3) more carefully screen and scrutinize phone calls, emails, and other communications to ensure that they are not being targeted in a social engineering or spear phishing attack; and (4) search for suitable identity theft protection and credit monitoring services, and pay to procure them.

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

89. As a result of Defendants' failures, Plaintiff and Class Members are at a substantial risk of suffering identity theft and fraud or misuse of their PII/PHI.

90. Plaintiff and the Class suffered actual injury from having PII/PHI compromised as a result of Defendants' negligent data management and resulting Data Breach including, but not limited to (a) damage to and diminution in the value of their PII/PHI, a form of property that Defendants obtained from Plaintiff; (b) violation of their privacy rights; and (c) present and increased risk arising from identity theft and fraud.

91. For the reasons mentioned above, Defendants' conduct, which allowed the Data

[43] Ben Kochman, *FBI, Secret Service Warn of Targeted Ransomware*, LAW360 (Nov. 18, 2019), https://www.law360.com/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware.

Breach to occur, caused Plaintiff and members of the Class these significant injuries and harm.

## CLASS ALLEGATIONS

92. Plaintiff brings this case individually and, pursuant to Rule 23 of the Federal Rules of Civil Procedure, on behalf of the following class:

> All individuals in the United States whose PII and/or PHI was compromised in the CHS/ CHSPSC Data Breach that occurred between on or about January 28 and January 30, 2023 (the "Class").

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

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

95. **Numerosity:** Plaintiff is informed and believes, and thereon alleges, that there are at minimum, millions of members of the Class described above. The exact size of the Class and the identities of the individual members are identifiable through Defendants' records, including but not limited to the files implicated in the Data Breach, but based on public information, the Class includes at least 1.1 million individuals.

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

a. Whether Defendants have a duty to protect the PII and PHI of Plaintiff and Class Members;

b. Whether Defendants were negligent in collecting and storing Plaintiff's and Class Members' PII and PHI, and breached their duties thereby;

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

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

97. **Typicality:** Plaintiff's claims are typical of the claims of the members of the Class. The claims of the Plaintiff and members of the Class are based on the same legal theories and arise from the same unlawful and willful conduct. Defendants were the custodian of Plaintiff's and Class Members' PII and PHI, when their PII and PHI was obtained by an unauthorized third party.

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

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

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

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

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

## FIRST CAUSE OF ACTION
## NEGLIGENCE
## (ON BEHALF OF PLAINTIFF AND THE CLASS)

103. Plaintiff restates and realleges paragraphs 1 through 102 above as if fully set forth herein.

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

105. Defendants' duty to use reasonable care arose from several sources, including but not limited to those described below.

106. Defendants 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 Defendants. By receiving, maintaining, and handling PII and PHI that is routinely targeted by criminals for unauthorized access, Defendants were obligated to act with reasonable care to protect against these foreseeable threats.

107. Defendants' duty also arose from Defendants' position as a healthcare provider. Defendants hold themselves out as a trusted provider of healthcare services, and thereby assuming a duty to reasonably protect the information it obtains from their patients. Indeed, Defendants, who receive, maintain, collect, and handle PII and PHI from their patients, were in a unique and superior position to protect against the harm suffered by Plaintiff and Class Members as a result of the Data Breach.

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

(g) failing to follow their own privacy policies and practices published to its patients; and (h) failing to adequately train and supervise employees and third party vendors with access or credentials to systems and databases containing sensitive PII or PHI.

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

110. As a direct and proximate result of Defendants' negligence, Plaintiff and Class Members have suffered injuries, including:

a. Theft of their PII and/or PHI;

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

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

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

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

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

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

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

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

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

## SECOND CAUSE OF ACTION
## NEGLIGENCE *PER SE*
## (ON BEHALF OF PLAINTIFF AND THE CLASS)

112. Plaintiff restates and realleges paragraphs 1 through 111 above as if fully set forth herein.

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

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

115. Defendants' violation of Section 5 of the FTC Act constitutes negligence *per se*.

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

117. Defendants are entities covered under the HIPAA, which sets minimum federal standards for privacy and security of PHI.

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

119. Specifically, HIPAA required Defendants to: (a) ensure the confidentiality, integrity, and availability of all electronic PHI they create, receive, maintain, or transmit; (b) identify and protect against reasonably anticipated threats to the security or integrity of the electronic PHI; (c) protect against reasonably anticipated, impermissible uses, or disclosures of the PHI; and (d) ensure compliance by their workforce to satisfy HIPAA's security requirements. 45 CFR § 164.102, *et. seq*.

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

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

122. Defendants' violation of HIPAA constitutes negligence *per se*.

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

124. As a direct and proximate result of Defendants' negligence, Plaintiff and Class Members have suffered injuries, including:

a. Theft of their PII and/or PHI;

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

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

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

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

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

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

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

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

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

## THIRD CAUSE OF ACTION
## DECLARATORY JUDGMENT
## (ON BEHALF OF PLAINTIFF AND THE CLASS)

126. Plaintiff restates and realleges paragraphs 1 through 125 above as if fully set forth herein.

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

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

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

a. Defendants owe a legal duty to secure patient PII and PHI obtained from their patients and to timely notify such patients of a data breach under the common law, Section 5 of the FTC Act, and HIPAA.

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

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

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

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

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

## PRAYER FOR RELIEF

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

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

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

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

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

e. Declaratory and injunctive relief as described herein;

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

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

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

**JURY TRIAL DEMANDED**

A jury trial is demanded on all claims so triable.

Dated: May 3, 2023

Respectfully submitted,

901Attorneys, LLC

s/ David A. McLaughlin
David A. McLaughlin, Esq. (015561)
200 Jefferson Avenue, Suite 900
Memphis, TN 38103
(901) 671-1551 phone
(901) 671-1571 fax
David@901Attorneys.com

– And –

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

**pro hac vice forthcoming*

*Attorneys for Plaintiff and Proposed Class*