IN THE UNITED STATES DISTRICT COURT
MIDDLE DISTRICT OF TENNESSEE

LOLA TATUM, RICHARD WALCK, and GLENDA G. CORN, individually and on behalf of all others similarly situated, Plaintiffs, v. CHSPSC, LLC, Defendant.	Case No. **CLASS ACTION** **JURY DEMAND**

CLASS ACTION COMPLAINT

Plaintiffs Lola Tatum, Richard Walck, and Glenda G. Corn ("Plaintiffs"), individually, and on behalf of all others similarly situated (collectively, "Class members"), by and through their attorneys, bring this Class Action Complaint against Defendant CHSPSC, LLC ("CHSPSC"), and complain and allege upon personal knowledge as to themselves and information and belief as to all other matters.

INTRODUCTION

1. Plaintiffs bring this class action against CHSPSC for its failure to secure and safeguard their and approximately 1,173,555 other individuals' personally identifying information ("PII") and personal health information ("PHI"), including names, dates of birth, addresses, medical billing and insurance information, medical diagnoses, prescription information, and Social Security numbers.

2. CHSPSC is a company that provides services to hospitals and clinics associated with Community Health Systems, Inc. ("Affiliates"). The company is headquartered in Franklin, Tennessee.

3. On February 2, 2023, CHSPSC was notified that Fortra, LLC ("Fortra"), the provider of a file transfer software used by CHSPSC, experienced a data breach between January 28, 2023 and January 30, 2023. Unauthorized individual(s) breached Fortra's network systems and accessed and acquired files containing the PII/PHI of CHSPSC's and its Affiliates' patients and employees, including Plaintiffs and Class members (the "Data Breach").

4. CHSPSC owed a duty to Plaintiffs and Class members to implement and maintain reasonable and adequate security measures to secure, protect, and safeguard their PII/PHI against unauthorized access and disclosure. CHSPSC breached that duty by, among other things, failing to implement and maintain reasonable security procedures and practices to protect its and its Affiliates' patients' and employees' PII/PHI from unauthorized access and disclosure.

5. As a result of CHSPSC's inadequate security and breach of its duties and obligations, the Data Breach occurred, and Plaintiffs' and Class members' PII/PHI was accessed and disclosed. This action seeks to remedy these failings and their consequences. Plaintiffs bring this action on behalf of themselves and all persons whose PII/PHI was exposed as a result of the Data Breach.

6. Plaintiffs, on behalf of themselves and all other Class members, assert claims for negligence, breach of fiduciary duty, breach of implied contract, and unjust enrichment, and seek declaratory relief, injunctive relief, monetary damages, statutory damages, punitive damages, equitable relief, and all other relief authorized by law.

PARTIES

Plaintiff Lola Tatum

7. Plaintiff Lola Tatum is a citizen of Mississippi.

8. Plaintiff Tatum obtained healthcare or related services from hospitals or clinics serviced by or affiliated with CHSPSC.

9. Plaintiff Tatum was previously employed by a CHSPSC Affiliate.

10. As a condition of receiving healthcare or related services, and in connection with her employment, CHSPSC required Plaintiff Tatum to provide CHSPSC with her PII/PHI.

11. Based on representations made by CHSPSC, Plaintiff Tatum believed that CHSPSC had implemented and maintained reasonable security and practices to protect her PII/PHI. With this belief in mind, Plaintiff Tatum provided her PII/PHI to CHSPSC in connection with her employment and in exchange for receiving healthcare or related services from CHSPSC.

12. In connection with employment and services provided to Plaintiff Tatum, CHSPSC stores and maintains Plaintiff Tatum's PII/PHI on its systems and transmitted the PII/PHI to third parties, including Fortra.

13. Plaintiff Tatum takes great care to protect her PII/PHI, including her Medicare information. Had Plaintiff Tatum known that CHSPSC does not adequately protect the PII/PHI in its possession, she would not have obtained or used services or employment from CHSPSC or its Affiliates or agreed to provide CHSPSC with her PII/PHI.

14. Plaintiff Tatum received a letter from CHSPSC notifying her that her PII/PHI was exposed in the Data Breach.

15. As a direct result of the Data Breach, Plaintiff Tatum has suffered injury and damages including, *inter alia*, a substantial and imminent risk of identity theft and medical identity theft; the wrongful disclosure and loss of confidentiality of her highly sensitive PII/PHI; deprivation of the value of her PII/PHI; and overpayment for services that did not include adequate data security.

Plaintiff Richard Walck

16. Plaintiff Richard Walck is a citizen of Mississippi.

17. Plaintiff Walck obtained healthcare or related services from hospitals or clinics serviced by or affiliated with CHSPSC. As a condition of receiving these services, CHSPSC required Plaintiff Walck to provide CHSPSC with his PII/PHI.

18. Based on representations made by CHSPSC, Plaintiff Walck believed that CHSPSC had implemented and maintained reasonable security and practices to protect his PII/PHI. With this belief in mind, Plaintiff Walck provided his PII/PHI to CHSPSC in connection with and in exchange for receiving healthcare or related services from CHSPSC.

19. In connection with services provided to Plaintiff Walck, CHSPSC stores and maintains Plaintiff Walck's PII/PHI on its systems and transmitted the PII/PHI to third-parties, including Fortra.

20. Plaintiff Walck takes great care to protect his PII/PHI. Had Plaintiff Walck known that CHSPSC does not adequately protect the PII/PHI in its possession, he would not have obtained or used services from CHSPSC or agreed to provide CHSPSC with his PII/PHI.

21. Plaintiff Walck received a letter from CHSPSC notifying him that his PII/PHI was exposed in the Data Breach.

22. As a direct result of the Data Breach, Plaintiff Walck has suffered injury and damages including, *inter alia*, a substantial and imminent risk of identity theft and medical identity theft; the wrongful disclosure and loss of confidentiality of his highly sensitive PII/PHI; deprivation of the value of his PII/PHI; and overpayment for services that did not include adequate data security.

Plaintiff Glenda G. Corn

23. Plaintiff Glenda G. Corn is a citizen of Florida.

24. Plaintiff Corn obtained healthcare or related services from hospitals or clinics serviced by or affiliated with CHSPSC. As a condition of receiving these services, CHSPSC required Plaintiff Corn to provide CHSPSC with her PII/PHI.

25. Based on representations made by CHSPSC, Plaintiff Corn believed that CHSPSC had implemented and maintained reasonable security and practices to protect her PII/PHI. With this belief in mind, Plaintiff Corn provided her PII/PHI to CHSPSC in connection with and in exchange for receiving healthcare or related services from CHSPSC.

26. In connection with services provided to Plaintiff Corn, CHSPSC stores and maintains Plaintiff Corn's PII/PHI on its systems and transmitted the PII/PHI to third parties, including Fortra.

27. Plaintiff Corn takes great care to protect her PII/PHI. Had Plaintiff Corn known that CHSPSC does not adequately protect the PII/PHI in its possession, she would not have obtained or used services from CHSPSC or its Affiliates or agreed to provide CHSPSC with her PII/PHI.

28. Plaintiff Corn received a letter from CHSPSC notifying her that her PII/PHI was exposed in the Data Breach.

29. As a direct result of the Data Breach, Plaintiff Corn has suffered injury and damages including, *inter alia*, a substantial and imminent risk of identity theft and medical identity theft; the wrongful disclosure and loss of confidentiality of her highly sensitive PII/PHI; deprivation of the value of her PII/PHI; and overpayment for services that did not include adequate data security.

Defendant CHSPSC, LLC

30. Defendant CHSPSC, LLC is a Delaware corporation with its principal place of business in Franklin, Tennessee. CHSPSC's headquarters are located at 4000 Meridian Blvd., Franklin, Tennessee 37067. CHSPSC may be served through its registered agent: Russell Baldwin, 4000 Meridian Blvd., Franklin, Tennessee 37067.

JURISDICTION AND VENUE

31. The Court has subject matter jurisdiction over Plaintiffs' claims under 28 U.S.C. § 1332(d)(2), because (a) there are 100 or more Class members, (b) at least one Class member is a citizen of a state that is diverse from CHSPSC, and (c) the matter in controversy exceeds $5,000,000, exclusive of interest and costs.

32. This Court has personal jurisdiction over CHSPSC because CHSPSC maintains its principal place of business in Tennessee.

33. Venue is proper in this District pursuant to 28 U.S.C. § 1391(b)(2) because CHSPSC's principal place of business is in this District and a significant amount of the events leading to Plaintiffs' causes of action occurred in this District.

FACTUAL ALLEGATIONS

Overview of CHSPSC

34. "CHSPSC is a professional services company that provides services to hospitals and clinics affiliated with Community Health Systems, Inc. ('CHSPSC Affiliates')," [1] including 78 hospitals in 15 states.[2] In the regular course of its business, CHSPSC collects and maintains the

[1] *Notice of Third-Party Security Incident Impacting CHSPSC Affiliate Data* ("Website Notice"), CMTY. HEALTH SYS., https://www.chs.net/notice-of-third-party-security-incident-impacting-chspsc-affiliate-data/ (last accessed Apr. 26, 2023).
[2] *Locations*, CMTY. HEALTH SYS., https://www.chs.net/serving-communities/locations/#USMap (last accessed Apr. 26, 2023).

PII/PHI of CHSPSC its and its Affiliates' patients and employees.

35. CHSPSC's Code of Conduct states that the company is "dedicated to compliance with all applicable federal, state, and local laws, rules, and regulations ('Applicable Law'), including privacy and security of patient health information."[3] CHSPSC acknowledges that "[p]atient information is highly confidential."[4] CHSPSC even states patient rights include "[p]ersonal privacy" and "privacy of health information."[5]

36. "When a patient enters a CHS affiliated facility, a large amount of personal, medical, and insurance data is collected."[6] The Code of Conduct states "[p]atient information may only be discussed or released as permitted or required under the Health Insurance Portability and Accountability Act ("HIPAA") or other privacy laws and in accordance with our HIPAA policies . . . which may require either a patient-directed request, a request from a patient's personal representative, or the express written authorization of the patient."[7]

37. Plaintiffs and Class members are, or were, patients or employees of CHSPSC or CHSPSC Affiliates and entrusted CHSPSC with their PII/PHI.[8]

The Data Breach

38. CHSPSC contracts with Fortra, a cybersecurity firm, for the use of a file transfer

[3] Community Health Systems, *Community Health Systems Code of Conduct* 3 (2023), https://www.chs.net/wp-content/uploads/Code-of-Conduct-January-2023-FINAL.pdf. The Code of Conduct applies to, and has been independently adopted by, each subsidiary of Community Health Systems, including CHSPSC. *See id.*
[4] *Id.* at 9.
[5] *Id.* at 11.
[6] *Id.* at 9.
[7] *Id.* at 10.
[8] CHSPSC's Website Notice states persons might be affected by the Data Breach include persons who "received services at one of the CHSPSC Affiliates, are a family member or guarantor with respect to a patient, or are a current or former employee of CHSPSC Affiliates." Website Notice, *supra* note 1.

software called "GoAnywhere."[9] CHSPSC uploads, stores, transfers, or accesses its or its Affiliates' patients' and employees' PII/PHI using GoAnywhere.

39. Between January 28, 2023 and January 30, 2023, an unauthorized individual, or unauthorized individuals, "used a previously unknown vulnerability to gain access to Fortra's systems, specifically Fortra's GoAnywhere file transfer service platform, compromising sets of files throughout Fortra's platform."[10] Fortra notified CHSPSC of the Data Breach on February 2, 2023.[11]

40. The Data Breach impacted the PII/PHI of certain persons who received services from CHSPSC or its Affiliates, family members or guarantors of patients of CHSPSC or its Affiliates, and current or former employees of CHSPSC or its Affiliates.[12]

41. CHSPSC began notifying affected persons on March 20, 2023.[13] CHSPSC's Website Notice states that the information that the cybercriminal accessed and acquired includes Class members' "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."[14]

CHSPSC Knew that Criminals Target PII/PHI

42. At all relevant times, CHSPSC knew, or should have known, that the PII/PHI that it collected was a target for malicious actors. Indeed, CHSPSC's parent company notes:

> A cyber-attack or security breach could result in the compromise of our facilities, confidential data or critical data systems and give rise to potential harm to patients, remediation and other expenses, expose us to liability under HIPAA, privacy and

[9] *Id.*
[10] *Id.*
[11] *Id.*
[12] *Id.*
[13] *See CHSPSC, LLC Data Breach Notification*, ME. ATT'Y GEN., https://apps.web.maine.gov/online/aeviewer/ME/40/e71fd844-b34a-449c-aba9-e4f63265f422.shtml (last accessed Apr. 26, 2023).
[14] Website Notice, *supra* note 1.

> data protection laws and regulations, consumer protection laws, common law or other theories, subject us to litigation and federal and state governmental inquiries, damage our reputation, and otherwise be disruptive to our business.[15]

CHSPSC's parent company further admits:

> [T]here can be no assurance that we, or our third-party vendors and providers, will not be subject to security breaches and other cybersecurity threats, including those related to the use of ransomware and other malicious software or other attempts by third parties to access, acquire, use, disclose, misappropriate or manipulate our information or disrupt our operations.[16]

43. CHSPSC's parent company recognizes "the volume and intensity of cyber-attacks on hospitals and health systems continues to increase," and admits it is "regularly the target of attempted cybersecurity and other threats that could have a security impact, and [it] expect[s] to continue to experience an increase in cybersecurity threats in the future."[17]

44. CHSPSC's parent company states, "We may be at increased risk because we outsource certain services or functions to, or have systems that interface with, third parties. Some of these third parties' information systems are also subject to [cyber-security] risks . . . and may store or have access to our data and may not have effective controls, processes, or practices to protect our information from attack, damage, or unauthorized access, acquisition, use or disclosure."[18]

45. CHSPSC's parent company knew that "[i]f [it] or any of [its] third-party service providers or certain other third-parties are subject to cyber-attacks or security or data breaches in the future, this could result in harm to patients . . . [and] the loss, misappropriation, corruption or unauthorized access, acquisition, use or disclosure of data."[19]

---

[15] Community Health Systems, *Form 10K* 42 (2022), https://chsnet.gcs-web.com/static-files/6a50aed5-21f9-474d-856c-d4fb8e595eab.
[16] *Id.*
[17] *Id.*
[18] *Id.* at 43.
[19] *Id.*

46. CHSPSC knew or should have known of these risks. Despite such knowledge, CHSPSC failed to implement and maintain reasonable and appropriate data privacy and security measures to protect Plaintiffs' and Class members' PII/PHI from cyber-attacks that CHSPSC should have anticipated and guarded against.

47. It is well known amongst companies that store sensitive personally identifying information that sensitive information—such as the Social Security numbers ("SSNs") and medical information stolen in the Data Breach—is valuable and frequently targeted by criminals. In a recent article, *Business Insider* noted that "[d]ata breaches are on the rise for all kinds of businesses, including retailers . . . . Many of them were caused by flaws in . . . systems either online or in stores."[20]

48. Cyber criminals seek out PHI at a greater rate than other sources of personal information. In a 2023 report, the healthcare compliance company Protenus found that there were 956 medical data breaches in 2022 with over 59 million patient records exposed.[21] This is an increase from the 758 medical data breaches which exposed approximately 40 million records that Protenus compiled in 2020.[22]

[20] Dennis Green, Mary Hanbury & Aine Cain, *If you bought anything from these 19 companies recently, your data may have been stolen*, BUS. INSIDER (Nov. 19, 2019, 8:05 A.M.), https://www.businessinsider.com/data-breaches-retailers-consumer-companies-2019-1.
[21] *See* PROTENUS, *2023 Breach Barometer*, PROTENUS.COM, https://www.protenus.com/breach-barometer-report (last accessed Apr. 26, 2023).
[22] *See id*.

49. PII/PHI is a valuable property right.[23] The value of PII/PHI as a commodity is measurable.[24] "Firms are now able to attain significant market valuations by employing business models predicated on the successful use of personal data within the existing legal and regulatory frameworks."[25] American companies are estimated to have spent over $19 billion on acquiring personal data of consumers in 2018.[26] 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.

50. As a result of the real and significant value of this material, identity thieves and other cyber criminals have openly posted credit card numbers, SSNs, 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 readily aggregated and become more valuable to thieves and more damaging to victims.

---

[23] *See* Marc van Lieshout, *The Value of Personal Data*, 457 INT'L FED'N FOR INFO. PROCESSING 26 (May 2015) ("The value of [personal] information is well understood by marketers who try to collect as much data about personal conducts and preferences as possible…"), https://www.researchgate.net/publication/283668023_The_Value_of_Personal_Data.

[24] *See* Robert Lowes, *Stolen EHR [Electronic Health Record] Charts Sell for $50 Each on Black Market*, MEDSCAPE.COM (April 28, 2014), http://www.medscape.com/viewarticle/824192.

[25] OECD, *Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value*, OECD ILIBRARY (April 2, 2013), https://www.oecd-ilibrary.org/science-and-technology/exploring-the-economics-of-personal-data_5k486qtxldmq-en.

[26] *See* IAB Data Center of Excellence, *U.S. Firms to Spend Nearly $19.2 Billion on Third-Party Audience Data and Data-Use Solutions in 2018, Up 17.5% from 2017*, IAB.COM (Dec. 5, 2018), https://www.iab.com/news/2018-state-of-data-report/.

51. PHI is particularly valuable and has been referred to as a "treasure trove for criminals."[27] A cybercriminal who steals a person's PHI can end up with as many as "seven to ten personal identifying characteristics of an individual."[28]

52. All-inclusive health insurance dossiers containing sensitive health insurance information, names, addresses, telephone numbers, email addresses, SSNs, and bank account information, complete with account and routing numbers, can fetch up to $1,200 to $1,300 each on the black market.[29] According to a report released by the Federal Bureau of Investigation's ("FBI") Cyber Division, criminals can sell healthcare records for 50 times the price of a stolen Social Security or credit card number.[30]

53. Criminals can use stolen PII/PHI to extort a financial payment by "leveraging details specific to a disease or terminal illness."[31] Quoting Carbon Black's Chief Cybersecurity Officer, one recent article explained: "Traditional criminals understand the power of coercion and extortion . . . By having healthcare information—specifically, regarding a sexually transmitted disease or terminal illness—that information can be used to extort or coerce someone to do what you want them to do."[32]

---

[27] *See* Andrew Steager, *What Happens to Stolen Healthcare Data*, HEALTHTECH MAGAZINE (Oct. 20, 2019), https://healthtechmagazine.net/article/2019/10/what-happens-stolen-healthcare-data-perfcon ("*What Happens to Stolen Healthcare Data*") (quoting Tom Kellermann, Chief Cybersecurity Officer, Carbon Black, stating "Health information is a treasure trove for criminals.").

[28] *Id.*

[29] *See* SC Staff, *Health Insurance Credentials Fetch High Prices in the Online Black Market*, SC MAG. (July 16, 2013), https://www.scmagazine.com/news/breach/health-insurance-credentials-fetch-high-prices-in-the-online-black-market.

[30] *See* 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.

[31] *What Happens to Stolen Healthcare Data*, *supra* note 27.

[32] *Id.*

54. Consumers place a high value on the privacy of that data, as they should. 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."[33]

55. 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.

Theft of PII/PHI Has Grave and Lasting Consequences for Victims

56. Theft of PII/PHI is serious. The FTC warns consumers that identity thieves use PII/PHI to exhaust financial accounts, receive medical treatment, start new utility accounts, and incur charges and credit in a person's name.[34]

57. Identity thieves use personal information for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.[35] According to Experian, one of the largest credit reporting companies in the world, "[t]he research shows that personal information is

[33] Janice Y. Tsai et al., *The Effect of Online Privacy Information on Purchasing Behavior*, *An Experimental Study*, 22(2) INFO. SYS. RSCH. 254 (June 2011) https://www.jstor.org/stable/23015560?seq=1.

[34] *See* Federal Trade Commission, *What to Know About Identity Theft*, FED. TRADE COMM'N CONSUMER INFO., https://www.consumer.ftc.gov/articles/what-know-about-identity-theft (last accessed Apr. 26, 2023).

[35] The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 12 C.F.R. § 1022.3(h). The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, social security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number." 12 C.F.R. § 1022.3(g).

valuable to identity thieves, and if they can get access to it, they will use it" to among other things: open a new credit card or loan; change a billing address so the victim no longer receives bills; open new utilities; obtain a mobile phone; open a bank account and write bad checks; use a debit card number to withdraw funds; obtain a new driver's license or ID; use the victim's information in the event of arrest or court action.[36]

58. With access to an individual's PII/PHI, criminals can do more than just empty a victim's bank account—they can also commit all manner of fraud, including: obtaining a driver's license or official identification card in the victim's name but with the thief's picture; using the victim's name and SSN to obtain government benefits; or, filing a fraudulent tax return using the victim's information. In addition, identity thieves may even give the victim's personal information to police during an arrest.[37]

59. Identity theft is not an easy problem to solve. In a survey, the Identity Theft Resource Center found that most victims of identity crimes need more than a month to resolve issues stemming from identity theft and some need over a year.[38]

60. Theft of SSNs also creates a particularly alarming situation for victims because those numbers cannot easily be replaced. In order to obtain a new number, a breach victim has to demonstrate ongoing harm from misuse of their SSN, and a new SSN will not be provided until after the harm has already been suffered by the victim.

---

[36] *See* Susan Henson, *What Can Identity Thieves Do with Your Personal Information and How Can You Protect Yourself*, EXPERIAN, https://www.experian.com/blogs/ask-experian/what-can-identity-thieves-do-with-your-personal-information-and-how-can-you-protect-yourself/ (last accessed Apr. 26, 2022).

[37] *See* Federal Trade Commission, *Warning Signs of Identity Theft*, IDENTITYTHEFT.GOV https://www.identitytheft.gov/Warning-Signs-of-Identity-Theft (last accessed Apr. 26, 2023).

[38] *See* Identity Theft Resource Center, *2021 Consumer Aftermath Report*, IDENTITY THEFT RES. CTR. (2021), https://www.idtheftcenter.org/identity-theft-aftermath-study/ (last accessed Apr. 26, 2022).

61. Due to the highly sensitive nature of SSNs, theft of SSNs in combination with other PII (e.g., name, address, date of birth) is akin to having a master key to the gates of fraudulent activity. TIME quotes data security researcher Tom Stickley, who is employed by companies to find flaws in their computer systems, as stating, "If I have your name and your Social Security number and you don't have a credit freeze yet, you're easy pickings."[39]

62. Theft of PII is even more serious when it includes theft of PHI. Data breaches involving medical information "typically leave[] a trail of falsified information in medical records that can plague victims' medical and financial lives for years."[40] It "is also more difficult to detect, taking almost twice as long as normal identity theft."[41] In warning consumers on the dangers of medical identity theft, the FTC states that an identity thief may use PII/PHI "to see a doctor, get prescription drugs, buy medical devices, submit claims with your insurance provider, or get other medical care." [42] The FTC also warns, "If the thief's health information is mixed with yours it could affect the medical care you're able to get or the health insurance benefits you're able to use."[43]

63. A report published by the World Privacy Forum and presented at the US FTC Workshop on Informational Injury describes what medical identity theft victims may experience:

- Changes to their health care records, most often the addition of falsified

[39] Patrick Lucas Austin, *'It Is Absurd.' Data Breaches Show it's Time to Rethink How We Use Social Security Numbers, Experts Say*, TIME (August 5, 2019), https://time.com/5643643/capital-one-equifax-data-breach-social-security/.
[40] Pam Dixon and John Emerson, *The Geography of Medical Identity Theft*, FTC.GOV (Dec. 12, 2017), http://www.worldprivacyforum.org/wp-content/uploads/2017/12/WPF_Geography_of_Medical_Identity_Theft_fs.pdf.
[41] *See* Federal Bureau of Investigation, *Health Care Systems and Medical Devices at Risk*…, *supra* note 30.
[42] *See What to Know About Medical Identity Theft*, FEDERAL TRADE COMMISSION CONSUMER INFORMATION, https://www.consumer.ftc.gov/articles/what-know-about-medical-identity-theft (last accessed Apr. 26, 2023).
[43] *Id*.

information, through improper billing activity or activity by imposters. These changes can affect the healthcare a person receives if the errors are not caught and corrected.

- Significant bills for medical goods and services neither sought nor received.
- Issues with insurance, co-pays, and insurance caps.
- Long-term credit problems based on problems with debt collectors reporting debt due to identity theft.
- Serious life consequences resulting from the crime; for example, victims have been falsely accused of being drug users based on falsified entries to their medical files; victims have had their children removed from them due to medical activities of the imposter; victims have been denied jobs due to incorrect information placed in their health files due to the crime.
- As a result of improper and/or fraudulent medical debt reporting, victims may not qualify for mortgage or other loans and may experience other financial impacts.
- Phantom medical debt collection based on medical billing or other identity information.
- Sales of medical debt arising from identity theft can perpetuate a victim's debt collection and credit problems, through no fault of their own.[44]

64. There may also be a time lag between when sensitive personal information is stolen, when it is used, and when a person discovers it has been used. For example, on average it takes approximately three months for consumers to discover their identity has been stolen and used, but it takes some individuals up to three years to learn that information.[45]

65. It is within this context that Plaintiffs and Class members must now live with the knowledge that their PII/PHI is forever in cyberspace and was taken by and in the possession of

[44] *See* Pam Dixon and John Emerson, *The Geography of Medical Identity Theft*, *supra* note 40.
[45] John W. Coffey, *Difficulties in Determining Data Breach Impacts*, 17 J. OF SYSTEMICS, CYBERNETICS AND INFORMATICS 9 (2019), http://www.iiisci.org/journal/pdv/sci/pdfs/IP069LL19.pdf.

people willing to use the information for any number of improper purposes and scams, including making the information available for sale on the black-market.

Damages Sustained by Plaintiffs and the Other Class Members

66. Plaintiffs and Class members have suffered and will suffer injury, including, but not limited to: (i) a substantially increased and imminent risk of identity theft; (ii) the compromise, publication, and theft of their PII/PHI; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from unauthorized use of their PII/PHI; (iv) lost opportunity costs associated with efforts attempting to mitigate the actual and future consequences of the Data Breach; (v) the continued risk to their PII/PHI which remains in CHSPSC's possession; (vi) future costs in terms of time, effort, and money that will be required to prevent, detect, and repair the impact of the PII/PHI compromised as a result of the Data Breach; and (vii) overpayment for the services that were received without adequate data security.

CLASS ALLEGATIONS

67. This action is brought and may be properly maintained as a class action pursuant to Rule 23 of the Federal Rules of Civil Procedure.

68. Plaintiffs bring this action on behalf of themselves and all members of the following Nationwide Class of similarly situated persons:

> All persons whose personally identifiable information or personal health information was compromised in the Data Breach by unauthorized persons, including all persons who were sent a notice of the Data Breach.

69. Excluded from the Class are CHSPSC, LLC and its affiliates, parents, subsidiaries, officers, agents, and directors, as well as the judge(s) presiding over this matter and the clerks of said judge(s).

70. Certification of Plaintiffs' claims for class-wide treatment is appropriate because Plaintiffs can prove the elements of their claims on a class-wide basis using the same evidence as would be used to prove those elements in individual actions alleging the same claims.

71. The members in the Class are so numerous that joinder of each of the Class members in a single proceeding would be impracticable. CHSPSC reported to the Maine Attorney General that approximately 1,173,555 persons' information was exposed in the Data Breach.[46]

72. Common questions of law and fact exist as to all Class members and predominate over any potential questions affecting only individual Class members. Such common questions of law or fact include, *inter alia*:

a. Whether CHSPSC had a duty to implement and maintain reasonable security procedures and practices to protect and secure Plaintiffs' and Class members' PII/PHI from unauthorized access and disclosure;

b. Whether CHSPSC had duties not to disclose the PII/PHI of Plaintiffs and Class members to unauthorized third parties;

c. Whether CHSPSC failed to exercise reasonable care to secure and safeguard Plaintiffs' and Class members' PII/PHI;

d. Whether an implied contract existed between Class members and CHSPSC, providing that CHSPSC would implement and maintain reasonable security measures to protect and secure Class members' PII/PHI from unauthorized access and disclosure;

e. Whether CHSPSC engaged in unfair, unlawful, or deceptive practices by failing to safeguard the PII/PHI of Plaintiffs and Class members;

f. Whether CHSPSC breached its duties to protect Plaintiffs' and Class members' PII/PHI; and

g. Whether Plaintiffs and Class members are entitled to damages and the measure of such damages and relief.

[46] *See Addendum to Previous Notification*, CSPSC (Apr. 17, 2023), available at https://apps.web.maine.gov/online/aeviewer/ME/40/810b151b-febe-43ef-9b77-b4c8ea0d9f4d.shtml (last accessed Apr. 26, 2023) (under "Notification and Protection Services" heading, click link titled "ME.pdf").

73. CHSPSC engaged in a common course of conduct giving rise to the legal rights sought to be enforced by Plaintiffs, on behalf of themselves and all other Class members. Individual questions, if any, pale in comparison, in both quantity and quality, to the numerous common questions that dominate this action.

74. Plaintiffs' claims are typical of the claims of the Class. Plaintiffs, like all proposed members of the Class, had their PII/PHI compromised in the Data Breach. Plaintiffs and Class members were injured by the same wrongful acts, practices, and omissions committed by CHSPSC, as described herein. Plaintiffs' claims therefore arise from the same practices or course of conduct that give rise to the claims of all Class members.

75. Plaintiffs will fairly and adequately protect the interests of the Class members. Plaintiffs are adequate representatives of the Class in that they have no interests adverse to, or that conflict with, the Class they seek to represent. Plaintiffs have retained counsel with substantial experience and success in the prosecution of complex consumer protection class actions of this nature.

76. A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. The damages and other financial detriment suffered by Plaintiffs and Class members are relatively small compared to the burden and expense that would be required to individually litigate their claims against CHSPSC, so it would be impracticable for Class members to individually seek redress from CHSPSC's wrongful conduct. Even if Class members could afford individual litigation, the court system could not. Individualized litigation creates a potential for inconsistent or contradictory judgments, and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management

difficulties and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court.

CAUSES OF ACTION

COUNT I
NEGLIGENCE

77. Plaintiffs reallege and incorporate by reference all preceding paragraphs as if fully set forth herein.

78. CHSPSC owed a duty to Plaintiffs and Class members to exercise reasonable care in safeguarding, securing, and protecting the PII/PHI in its possession, custody, or control.

79. CHSPSC knew or should have known the risks of collecting and storing Plaintiffs' and all other Class members' PII/PHI and the importance of maintaining and using secure systems. CHSPSC knew or should have known of the many data breaches that have targeted companies that stored PII/PHI in recent years.

80. Given the nature of CHSPSC's business, the sensitivity and value of the PII/PHI it maintains, and the resources at its disposal, CHSPSC should have identified and foreseen that the third parties it contracts with could have vulnerabilities in their systems and prevented the dissemination of Plaintiffs' and Class members' PII/PHI.

81. CHSPSC makes explicit statements on its website that it is aware of the risk of potential data breaches, that it will follow privacy laws and regulations, and that it will use reasonable methods to protect the PII/PHI in its control.

82. CHSPSC breached these duties by failing to exercise reasonable care in safeguarding and protecting Plaintiffs' and Class members' PII/PHI by failing to ensure that the third-parties that it shares PII/PHI with design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures,

protocols, and software and hardware systems to safeguard and protect PII/PHI entrusted to them—including Plaintiffs' and Class members' PII/PHI.

83. Plaintiffs and Class members had no ability to protect their PII/PHI that was, or remains, in CHSPSC's possession.

84. It was or should have been reasonably foreseeable to CHSPSC that its failure to exercise reasonable care in safeguarding and protecting Plaintiffs' and Class members' PII/PHI by failing to ensure that the third-parties that it shares PII/PHI with design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems would result in the unauthorized release, disclosure, and dissemination of Plaintiffs' and Class members' PII/PHI to unauthorized individuals.

85. But for CHSPSC's negligent conduct or breach of the above-described duties owed to Plaintiffs and Class members, their PII/PHI would not have been compromised. The PII/PHI of Plaintiffs and the Class was lost and accessed as the proximate result of CHSPSC's failure to exercise reasonable care in safeguarding, securing, and protecting such PII/PHI by, *inter alia*, ensuring that third parties it contracts with and shares PII/PHI with adopt, implement, and maintain appropriate security measures.

86. As a result of CHSPSC's above-described wrongful actions, inaction, and want of ordinary care that directly and proximately caused the Data Breach, Plaintiffs and Class members have suffered and will suffer injury, including, but not limited to: (i) a substantially increased and imminent risk of identity theft; (ii) the compromise, publication, and theft of their PII/PHI; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from unauthorized use of their PII/PHI; (iv) lost opportunity costs associated with efforts

attempting to mitigate the actual and future consequences of the Data Breach; (v) the continued risk to their PII/PHI which remains in CHSPSC's possession; (vi) future costs in terms of time, effort, and money that will be required to prevent, detect, and repair the impact of the PII/PHI compromised as a result of the Data Breach; and (vii) overpayment for the services that were received without adequate data security.

COUNT II
NEGLIGENCE PER SE

87. Plaintiffs reallege and incorporate by reference all preceding paragraphs as if fully set forth herein.

88. CHSPSC's duties arise from, *inter alia*, the HIPAA Privacy Rule ("Standards for Privacy of Individually Identifiable Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and E, and the HIPAA Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C (collectively, "HIPAA Privacy and Security Rules").

89. CHSPSC's duties also arise from Section 5 of the FTC Act ("FTCA"), 15 U.S.C. § 45(a)(1), which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted by the FTC, the unfair act or practice by businesses, such as CHSPSC, of failing to employ reasonable measures to protect and secure PII/PHI.

90. CHSPSC violated HIPAA Privacy and Security Rules and Section 5 of the FTCA by failing to ensure that third parties it contracts with and shares PII/PHI with use reasonable measures to protect Plaintiffs' and all other Class members' PII/PHI and comply with applicable industry standards. CHSPSC's conduct was particularly unreasonable given the nature and amount of PII/PHI it obtains and stores, and the foreseeable consequences of a

data breach involving PII/PHI including, specifically, the substantial damages that would result to Plaintiffs and the other Class members.

91. CHSPSC's violations of HIPAA Privacy and Security Rules and Section 5 of the FTCA constitutes negligence per se.

92. Plaintiffs and Class members are within the class of persons that HIPAA Privacy and Security Rules and Section 5 of the FTCA were intended to protect.

93. The harm occurring as a result of the Data Breach is the type of harm HIPAA Privacy and Security Rules and Section 5 of the FTCA were intended to guard against.

94. It was, or should have been, reasonably foreseeable to CHSPSC that its failure to exercise reasonable care in safeguarding and protecting Plaintiffs' and Class members' PII/PHI by failing to ensure that the third-parties that it contracts with and shares PII/PHI with design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems, would result in the release, disclosure, and dissemination of Plaintiffs' and Class members' PII/PHI to unauthorized individuals.

95. The injury and harm that Plaintiffs and the other Class members suffered was the direct and proximate result of CHSPSC's violations of HIPAA Privacy and Security Rules and Section 5 of the FTCA.

96. Plaintiffs and Class members have suffered (and will continue to suffer) economic damages and other injury and actual harm in the form of, *inter alia*: (i) a substantially increased and imminent risk of identity theft and medical identity theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (ii) improper disclosure of their PII/PHI; (iii) breach of the confidentiality of

their PII/PHI; (iv) deprivation of the value of their PII/PHI, for which there is a well-established national and international market; (v) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of medical identity theft they face and will continue to face; and (vi) overpayment for the services that were received without adequate data security.

COUNT III
BREACH OF FIDUCIARY DUTY

97. Plaintiffs reallege and incorporate by reference all preceding paragraphs as if fully set forth herein.

98. As a condition of obtaining services or employment from CHSPSC, Plaintiffs and Class members gave CHSPSC their PII/PHI in confidence, believing that CHSPSC would protect that information. Plaintiffs and Class members would not have provided CHSPSC with this information had they known it would not be adequately protected. CHSPSC's acceptance and storage of Plaintiffs' and Class members' PII/PHI created a fiduciary relationship between CHSPSC and Plaintiffs and Class members. In light of this relationship, CHSPSC must act primarily for the benefit of its and its Affiliates' patients and employees, which includes safeguarding and protecting Plaintiffs' and Class Members' PII/PHI.

99. CHSPSC has a fiduciary duty to act for the benefit of Plaintiffs and Class members upon matters within the scope of their relationship. It breached that duty by failing to ensure that the third-parties it contracts with and shares PII/PHI with properly protect the integrity of the system containing Plaintiffs' and Class members' PII/PHI, failing to comply with the data security guidelines set forth by HIPAA, and otherwise failing to safeguard Plaintiffs' and Class members' PII/PHI that it collected.

100. As a direct and proximate result of CHSPSC's breach of its fiduciary duties, Plaintiffs and Class members have suffered and will suffer injury, including, but not limited to: (i) a substantially increased and imminent risk of identity theft; (ii) the compromise, publication, and theft of their PII/PHI; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from unauthorized use of their PII/PHI; (iv) lost opportunity costs associated with efforts attempting to mitigate the actual and future consequences of the Data Breach; (v) the continued risk to their PII/PHI which remains in CHSPSC's possession; (vi) future costs in terms of time, effort, and money that will be required to prevent, detect, and repair the impact of the PII/PHI compromised as a result of the Data Breach; and (vii) overpayment for the services that were received without adequate data security.

COUNT IV
BREACH OF IMPLIED CONTRACT

101. Plaintiffs reallege and incorporate by reference all preceding paragraphs as if fully set forth herein.

102. In connection with receiving health care services or employment, Plaintiffs and all other Class members entered into implied contracts with CHSPSC.

103. Pursuant to these implied contracts, Plaintiffs and Class members benefited CHSPSC, directly or through a CHSPSC Affiliate, through their labor or by paying monies to CHSPSC, and provided CHSPSC with their PII/PHI. In exchange, CHSPSC agreed to, among other things, and Plaintiffs understood that CHSPSC would: (1) provide products, services, or employment, to Plaintiffs and Class members; (2) take reasonable measures to protect the security and confidentiality of Plaintiffs' and Class members' PII/PHI; (3) protect Plaintiffs' and Class members' PII/PHI in compliance with federal and state laws and regulations and industry standards; and (4) ensure third parties it contracts with and provides PII/PHI to

implement and maintain reasonable measures to protect the security and confidentiality of Plaintiffs' and Class members' PII/PHI.

104. The protection of PII/PHI was a material term of the implied contracts between Plaintiffs and Class members, on the one hand, and CHSPSC, on the other hand. Indeed, as set forth *supra*, CHSPSC recognized the importance of data security and the privacy of its and its Affiliates' patients' and employees' PII/PHI. Had Plaintiffs and Class members known that CHSPSC would not adequately protect their PII/PHI, they would not have paid for products or services or obtained employment from CHSPSC.

105. Plaintiffs and Class members performed their obligations under the implied contract when they provided CHSPSC with their PII/PHI and paid for products and services from CHSPSC or its Affiliates, or completed work for CHSPSC or its Affiliates, expecting that their PII/PHI would be protected.

106. CHSPSC breached its obligations under its implied contracts with Plaintiffs and Class members by failing to implement and maintain reasonable security measures to protect and secure their PII/PHI, and in failing to ensure that third-parties it contracts with and shares PII/PHI with implement and maintain security protocols and procedures to protect Plaintiffs' and Class members' PII/PHI in a manner that complies with applicable laws, regulations, and industry standards.

107. CHSPSC's breach of its obligations of the implied contracts with Plaintiffs and Class members directly resulted in the Data Breach and the resulting injuries to Plaintiffs and Class members.

108. Plaintiffs and all other Class members were damaged by CHSPSC's breach of implied contracts because: (i) they paid monies (directly or through their insurers or CHSPSC

Affiliates) or provided labor in exchange for data security protection they did not receive; (ii) they now face a substantially increased and imminent risk of identity theft and medical identity theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (iii) their PII/PHI was improperly disclosed to unauthorized individuals; (iv) the confidentiality of their PII/PHI has been breached; (v) they were deprived of the value of their PII/PHI, for which there is a well-established national and international market; (vi) they lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of medical identity theft they face and will continue to face; and (vii) they overpaid for the services that were received without adequate data security.

COUNT V
UNJUST ENRICHMENT

109. Plaintiffs reallege and incorporate by reference paragraphs 1–76 as if fully set forth herein.

110. This claim is pleaded in the alternative to the breach of implied contract claim.

111. In obtaining services or employment from CHSPSC, Plaintiffs and Class members provided and entrusted their PII and PHI to CHSPSC.

112. Plaintiffs and Class members conferred a monetary benefit upon CHSPSC in the form of monies paid for products or services or via the value of their labor (including by facilitating payments to CHSPSC), with an implicit understanding that CHSPSC would use some of its revenue to protect the PII/PHI it collects.

113. CHSPSC accepted or had knowledge of the benefits conferred upon it by Plaintiffs and Class Members. CHSPSC benefitted from the receipt of Plaintiffs' and Class members' PII/PHI, as this was used to facilitate billing and payment services, as well as from Plaintiffs' and Class members' labor, which enabled CHSPSC to carry out its business.

114. As a result of CHSPSC's conduct, Plaintiffs and Class members suffered actual damages in an amount equal to the difference in value between their payments or labor made with reasonable data privacy and security practices and procedures that Plaintiffs and Class members paid for and expected, and those payments and labor without reasonable data privacy and security practices and procedures that they received.

115. CHSPSC should not be permitted to retain the money belonging to Plaintiffs and Class members because CHSPSC failed to adequately implement the data privacy and security procedures for itself and the third parties that it contracts with and shares PII/PHI with that Plaintiffs and Class members paid for and expected, and that were otherwise mandated by federal, state, and local laws and industry standards.

116. CHSPSC should be compelled to provide for the benefit of Plaintiffs and Class members all unlawful proceeds it received as a result of the conduct and Data Breach alleged herein.

PRAYER FOR RELIEF

Plaintiffs, individually and on behalf of all other members of the Class, respectfully request that the Court enter judgment in their favor and against CHSPSC as follows:

A. Certifying the Class as requested herein, designating Plaintiffs as Class representatives, and appointing Plaintiffs' counsel as Class Counsel;

B. Awarding Plaintiffs and the Class appropriate monetary relief, including actual damages, statutory damages, punitive damages, restitution, and disgorgement;

C. Awarding Plaintiffs and the Class equitable, injunctive, and declaratory relief, as may be appropriate. Plaintiffs, on behalf of themselves and the Class, seek appropriate injunctive relief designed to prevent CHSPSC from experiencing another data breach by

adopting and implementing best data security practices to safeguard PII/PHI and to provide or extend credit monitoring services and similar services to protect against all types of identity theft and medical identity theft;

D. Awarding Plaintiffs and the Class pre-judgment and post-judgment interest to the maximum extent allowable;

E. Awarding Plaintiffs and the Class reasonable attorneys' fees, costs, and expenses, as allowable; and

F. Awarding Plaintiffs and the Class such other favorable relief as allowable under law.

JURY TRIAL DEMANDED

Plaintiffs demand a trial by jury of all claims in this Class Action Complaint so triable.

Dated: April 26, 2023

Respectfully submitted,

/s/ Kevin Sharp

Kevin H. Sharp, BPR No. 016287
Leigh Anne St. Charles, BPR No. 036945
SANFORD HEISLER SHARP, LLP
611 Commerce Street, Suite 3100
Nashville, TN 37203
Telephone: (615) 434-7000
Facsimile: (615) 434-7020
ksharp@sanfordheisler.com
lstcharles@sanfordheisler.com

Ben Barnow*
Anthony L. Parkhill*
Riley W. Prince*
Barnow and Associates, P.C.
205 West Randolph Street, Ste. 1630
Chicago, IL 60606
Tel: 312-621-2000
Fax: 312-641-5504
b.barnow@barnowlaw.com
aparkhill@barnowlaw.com

rprince@barnowlaw.com

Counsel for Plaintiffs

* *Pro hac vice forthcoming*