IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF OHIO
DAYTON DIVISION

DWAYNE COOPER, individually, and on behalf of all others similarly situated, **Plaintiff,** **vs.** **CARESOURCE,** **Defendant.**	**Case No.** **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiff Dwayne Cooper ("Plaintiff" or "Cooper"), individually and on behalf of all others similarly situated brings this Class Action Complaint against Defendant CareSource ("Defendant" or "CareSource") and alleges as follows.

INTRODUCTION

1. Plaintiff brings this class action against CareSource for its failure to secure and safeguard the personally identifying information ("PII") and personal health information ("PHI") of over three million people that it was entrusted to safeguard. As a result of its failure to do so as described below, the following types of personal information are now in the hands of criminal hackers: names, addresses, birthdates, Social Security numbers, and sensitive medical information including "health conditions," "medications," "allergies," and "diagnosis."

2. CareSource provides healthcare coverage and is one of the country's largest Medicaid managed care plans.[1] The company's website states that it is "required by law to keep

[1] https://www.caresource.com/about-us/ (last visited Sept. 3, 2023).

the privacy and security of your protected health information."[2] CareSource states that it "protect[s] our members' health information in many ways" and promises to "let you know quickly if a breach occurs that may have compromised the privacy or security of your information."[3]

3. According to CareSource's website, the software of one of its vendors "was hacked by a bad actor" on May 31, 2023.[4] By June 1, 2023, CareSource had become aware of the breach and "patched the software."[5] Yet it was not until August 24, 2023 that it began notifying its members, including Cooper, that their data was "stolen by the bad actor."[6]

4. CareSource owed a non-delegable duty to Cooper 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. It also had an obligation to ensure that any vendor or third party it selected to offload the sensitive information it was entrusted with would take reasonable measures to safeguard that data.

5. As a result of CareSource's inadequate vendor screening, security measures and breach of its legal duties and obligations, the aforementioned data breach occurred, and Cooper's and Class Members' PII/PHI was accessed and "stolen" by an unspecified "bad actor." CareSource permitted Plaintiffs' and Class Members' PII/PHI to be held in unencrypted form despite the heightened sensitivity of such PII/PHI.

---

[2] https://www.caresource.com/about-us/legal/hipaa-privacy-practices/hipaa-privacy-practices-ohio-medicaid/ (last visited Sept. 3, 2023).

[3] *Id.*

[4] https://www.caresource.com/about-us/legal/corporate-compliance/vendor-compliance/hipaa-hitech/cybersecurity-incident/ (last visited Sept. 3, 2023).

[5] *Id.*

[6] *Id.*

6. Cooper, on behalf of himself and all other Class Members, asserts claims herein against CareSource for negligence, negligence *per se*, breach of fiduciary duty, breach of implied contract, breach of contracts to which Plaintiff and Class Members are intended third party beneficiaries, violations of the West Virginia Consumer Credit Protection Act, and, alternatively, unjust enrichment.

PARTIES

7. Plaintiff Dwayne Cooper is a resident of Chester in West Virginia. He received a letter from CareSource dated August 24, 2023 which stated that "some of your protected health information was part of the data stolen by the bad actor."

8. Plaintiff Cooper takes great care to protect his PII/PHI. Had Cooper known that CareSource would not adequately protect the PII/PHI entrusted to it, he would not have obtained or used services from CareSource or agreed to provide CareSource with his PII/PHI.

9. As a direct result of the Data Breach, Plaintiff Cooper 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. He has also spent significant time monitoring his accounts for fraudulent activity, and will need to do so for the foreseeable future.

10. Defendant CareSource is an Ohio corporation that maintains its headquarters at 230 N. Main Street, Dayton, Ohio 45402.

JURISDICTION AND VENUE

11. The Court has subject matter jurisdiction over this action pursuant to the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million,

exclusive of interest and costs. The number of class members exceeds 100, many of whom have different citizenship from CareSource, including certain Plaintiff. Thus, minimal diversity exists under 28 U.S.C. § 1332(d)(2)(A).

12. This Court has personal jurisdiction over CareSource because its principal place of business is in this District.

13. Venue is proper in this District because CareSource's principal place of business is in this District and a significant amount of the events leading to Plaintiff's causes of action occurred in this District.

FACTUAL ALLEGATIONS

Overview of CareSource's Data Breach

14. CareSource was founded in 1989 on the premise of providing quality health care coverage for Medicaid consumers.[7] It is now one of the nation's largest Medicaid managed care plans. CareSource also offers private health insurance plans on the Health Insurance Marketplace, including Medicare Advantage and MyCare Ohio plans. CareSource has more than 1.9 million members across five states.

15. In the course of its ordinary business operations, CareSource is entrusted with safeguarding the sensitive PII and PHI of its members.

16. As noted above, the software of one of CareSource's vendors was "hacked by a bad actor" on May 31, 2023.[8] CareSource claims that it uses the vendor's software to "share data to manage your benefits."[9]

---

[7] https://smartfinancial.com/health-companies/caresource-insurance (last visited Sept. 3, 2023).

[8] https://www.caresource.com/about-us/legal/corporate-compliance/vendor-compliance/hipaa-hitech/cybersecurity-incident/ (last visited Sept. 3, 2023).

[9] *Id.*

17. CareSource stated that, upon learning of the breach, it "patched the software as instructed by MOVEit on June 1."[10] CareSource undertook an investigation which "found that the bad actor did access the software on May 31. They copied certain data from the server. It also found that the bad actor lost access to the software when the patch was added."[11]

18. CareSource's website now states that "[w]e are sorry to say that some of your protected health information was part of the data stolen by the bad actor."[12]

CareSource Knew that Criminals Target PII/PHI

19. CareSource knew that the sensitive personal data with which it was entrusted would be a lucrative target for hackers. Despite such knowledge, CareSource and its vendor both failed to implement and maintain reasonable and appropriate data privacy and security measures to protect Plaintiff's and Class Members' PII/PHI from cyber-attacks that CareSource should have anticipated and guarded against.

20. 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."[13]

---

[10] *Id.*

[11] *Id.*

[12] *Id.*

[13] 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. 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.[14] This is an increase from the 758 medical data breaches which exposed approximately 40 million records that Protenus compiled in 2020.[15]

22. PII/PHI is a valuable property right.[16] The value of PII/PHI as a commodity is measurable.[17] "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."[18] American companies are estimated to have spent over $19 billion on acquiring personal data of consumers in 2018.[19] 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.

23. 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

---

[14] *See* PROTENUS, *2023 Breach Barometer*, PROTENUS.COM, https://www.protenus.com/breach-barometer-report (last accessed Apr. 26, 2023).

[15] *See id.*

[16] *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.

[17] *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.

[18] 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.

[19] *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/.

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.

24. PHI is particularly valuable and has been referred to as a "treasure trove for criminals."[20] A cybercriminal who steals a person's PHI can end up with as many as "seven to ten personal identifying characteristics of an individual."[21]

25. 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.[22] 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.[23]

26. Criminals can use stolen PII/PHI to extort a financial payment by "leveraging details specific to a disease or terminal illness."[24] Quoting Carbon Black's Chief Cybersecurity Officer, one recent article explained: "Traditional criminals understand the power of coercion and

---

[20] *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.").

[21] *Id.*

[22] *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.

[23] *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.

[24] *What Happens to Stolen Healthcare Data*, *supra* note 42.

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."[25]

27. 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."[26]

28. 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

29. 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.[27]

---

[25] *Id.*

[26] 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.

[27] *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).

30. Identity thieves use personal information for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.[28] Experian, one of the largest credit reporting companies in the world, warns consumers that "[i]dentity thieves can profit off your personal information" by, among other things, selling the information, taking over accounts, using accounts without permission, applying for new accounts, obtaining medical procedures, filing a tax return, and applying for government benefits.[29]

31. 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.[30]

[28] 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).

[29] *See* Louis DeNicola, *What Can Identity Thieves Do with Your Personal Information and How Can You Protect Yourself*, EXPERIAN (May 21, 2023), https://www.experian.com/blogs/ask-experian/what-can-identity-thieves-do-with-your-personal-information-and-how-can-you-protect-yourself/.

[30] *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).

32. 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.[31]

33. 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.

34. 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."[32]

35. 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."[33] It "is also more difficult to detect, taking almost twice as long as normal identity theft."[34] In warning consumers on the dangers of

---

[31] *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).

[32] 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/.

[33] 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.

[34] *See* Federal Bureau of Investigation, *Health Care Systems and Medical Devices at Risk*…, *supra* note 45.

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." [35] 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."[36]

36. 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 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

[35] *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).

[36] *Id*.

collection and credit problems, through no fault of their own.[37]

37. 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.[38]

38. It is within this context that Plaintiff 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 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 Plaintiff and the Other Class Members

39. Plaintiff 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 CareSource'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) loss of value of

[37] *See* Pam Dixon and John Emerson, *The Geography of Medical Identity Theft*, *supra* note 55.

[38] 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.

their PII/PHI, for which there is a well-established national and international market; and (viii) overpayment for the services that were received without adequate data security.

CLASS ALLEGATIONS

40. This action is brought and may be properly maintained as a class action pursuant to Fed. R. Civ. P. 23(a), 23(b)(2) and 23(b)(3).

41. Plaintiff brings this action on behalf of himself and all members of the following 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.

42. Excluded from the Class are CareSource and their affiliates, parents, subsidiaries, officers, agents, and directors, as well as the judge(s) presiding over this matter and the clerks of said judge(s).

43. Certification of Plaintiff's claims for class-wide treatment is appropriate because Plaintiff 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.

44. The members of the Class are so numerous that joinder of each of the Class Members in a single proceeding would be impracticable. CareSource has reported to the U.S. Department of that the breach impacted 3,180,537 people.[39]

45. 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 either or both CareSource and its vendor had a duty to implement and maintain reasonable security procedures and practices to protect and secure

[39] https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (last visited Sept. 3, 2023).

Plaintiff's and Class Members' PII/PHI from unauthorized access and disclosure;

b. Whether either or both CareSource and its vendor had duties not to disclose the PII/PHI of Plaintiff and Class Members to unauthorized third parties;

c. Whether either or both CareSource and its vendor failed to exercise reasonable care to secure and safeguard Plaintiff's and Class Members' PII/PHI;

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

e. Whether CareSource engaged in unfair, unlawful, or deceptive practices by failing to safeguard the PII/PHI of Plaintiff and Class Members;

f. Whether CareSource breached its duties to protect Plaintiff's and Class Members' PII/PHI; and

g. Whether Plaintiff and Class Members are entitled to damages and the measure of such damages and relief.

46. CareSource in a common course of conduct giving rise to the legal rights sought to be enforced by Plaintiff, 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.

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

48. Plaintiff will fairly and adequately protect the interests of the Class Members. Plaintiff Cooper is an adequate representative of the Class in that he has no interests adverse to, or that conflict with, the Class he seeks to represent. Plaintiff has retained counsel with

substantial experience and success in the prosecution of complex consumer protection class actions of this nature.

49. 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 Plaintiff and Class Members are relatively small compared to the burden and expense that would be required to individually litigate their claims against CareSource, so it would be impracticable for Class Members to individually seek redress from CareSource'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

50. Plaintiff reallege and incorporate by reference all preceding paragraphs as if fully set forth herein.

51. CareSource owed a duty to Plaintiff and Class Members to exercise reasonable care in safeguarding, securing, and protecting the PII/PHI in its possession, custody, or control. This duty extended to any vendor selected by CareSource to be entrusted with the sensitive data of Plaintiff and Class Members.

52. CareSource knew or should have known the risks of collecting and storing Plaintiff's and all other Class Members' PII/PHI and the importance of maintaining and using

secure systems. CareSource knew or should have known of the many data breaches that have targeted companies that stored PII/PHI in recent years.

53. Given the nature of CareSource's business, the sensitivity and value of the PII/PHI it maintains, and the resources at its disposal, CareSource should have identified and foreseen that the third parties with whom it contracts could have vulnerabilities in its systems and prevented the dissemination of Plaintiff's and Class Members' PII/PHI.

54. CareSource breached these duties by failing to exercise reasonable care in safeguarding and protecting Plaintiff's 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 Plaintiff's and Class Members' PII/PHI.

55. Plaintiff and Class Members had no ability to protect their PII/PHI that was, or remains, in CareSource's possession.

56. It was or should have been reasonably foreseeable to CareSource that its failure to exercise reasonable care in safeguarding and protecting Plaintiff's 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 Plaintiff's and Class Members' PII/PHI to unauthorized individuals.

57. But for CareSource's negligent conduct or breach of the above-described duties owed to Plaintiff and Class Members, their PII/PHI would not have been compromised. The

PII/PHI of Plaintiff and the Class was lost and accessed as the proximate result of CareSource'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.

58. As a result of CareSource's above-described wrongful actions, inaction, and want of ordinary care that directly and proximately caused the Data Breach, Plaintiff 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 CareSource'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) loss of value of their PII/PHI, for which there is a well-established national and international market; and (viii) overpayment for the services that were received without adequate data security.

COUNT II
NEGLIGENCE *PER SE*

59. Plaintiff realleges and incorporate by reference all preceding paragraphs as if fully set forth herein.

60. CareSource'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").

61. CareSource'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 CareSource, of failing to employ reasonable measures to protect and secure PII/PHI.

62. CareSource 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 Plaintiff's and all other Class Members' PII/PHI and comply with applicable industry standards. CareSource's conduct was particularly unreasonable given the nature and amount of PII/PHI they obtain and store, and the foreseeable consequences of a data breach involving PII/PHI including, specifically, the substantial damages that would result to Plaintiff and the other Class Members.

63. CareSource's violations of HIPAA Privacy and Security Rules and Section 5 of the FTCA constitutes negligence *per se*.

64. Plaintiff 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.

65. 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.

66. It was, or should have been, reasonably foreseeable to CareSource that its failure to exercise reasonable care in safeguarding and protecting Plaintiff's 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 Plaintiff's and Class Members' PII/PHI to unauthorized individuals.

67. The injury and harm that Plaintiff and the other Class Members suffered was the direct and proximate result of CareSource's violations of HIPAA Privacy and Security Rules and Section 5 of the FTCA.

68. Plaintiff and Class Members have suffered and will suffer injury, including, but not limited: (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 CARESOURCE'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; (vii) loss of value of their PII/PHI, for which there is a well-established national and international market; and (viii) overpayment for the services that were received without adequate data security.

COUNT III
BREACH OF FIDUCIARY DUTY

69. Plaintiff realleges and incorporate by reference all preceding paragraphs as if fully set forth herein.

70. As a condition of obtaining services or employment from CareSource, Plaintiff and Class Members gave CareSource their PII/PHI in confidence, believing that it would protect that information. Plaintiff and Class Members would not have provided CareSource

with this information had they known it would not be adequately protected. CareSource's acceptance and storage of Plaintiff's and Class Members' PII/PHI created a fiduciary relationship between CareSource and Plaintiff and Class Members. In light of this relationship, CareSource must act primarily for the benefit of its and its affiliates' patients and employees, which includes safeguarding and protecting Plaintiff's and Class Members' PII/PHI.

71. CareSource has a fiduciary duty to act for the benefit of Plaintiff 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 share PII/PHI with properly protect the integrity of the system containing Plaintiff's and Class Members' PII/PHI, failing to comply with the data security guidelines set forth by HIPAA, and otherwise failing to safeguard Plaintiff's and Class Members' PII/PHI that it collected.

72. As a direct and proximate result of CareSource's breach of its fiduciary duties, Plaintiff 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 CareSource'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; (vii) loss of value of their PII/PHI, for which there is a well-established

national and international market; and (viii) overpayment for the services that were received without adequate data security.

COUNT IV
BREACH OF IMPLIED CONTRACT

73. Plaintiff realleges and incorporate by reference all preceding paragraphs as if fully set forth herein.

74. In connection with receiving health care services or employment, Plaintiff and all other Class Members entered into implied contracts with CareSource.

75. Pursuant to these implied contracts, Plaintiff and Class Members benefited CareSource, directly or through an affiliate, through their labor or by paying monies to CareSource, and provided CareSource with their PII/PHI. In exchange, CareSource agreed to, among other things, and Plaintiff understood that CareSource would: (1) provide products, services, or employment, to Plaintiff and Class Members; (2) take reasonable measures to protect the security and confidentiality of Plaintiff's and Class Members' PII/PHI; (3) protect Plaintiff's 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 provide PII/PHI to implement and maintain reasonable measures to protect the security and confidentiality of Plaintiff's and Class Members' PII/PHI.

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

77. Plaintiff and Class Members performed their obligations under the implied contract when they provided CareSource with their PII/PHI and paid for products and services from CareSource or its affiliates, or completed work for CareSource or its affiliates, expecting that their PII/PHI would be protected.

78. CareSource breached its obligations under its implied contracts with Plaintiff 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 share PII/PHI with implement and maintain security protocols and procedures to protect Plaintiff's and Class Members' PII/PHI in a manner that complies with applicable laws, regulations, and industry standards.

79. CareSource's breach of its obligations of the implied contracts with Plaintiff and Class Members directly resulted in the Data Breach and the resulting injuries to Plaintiff and Class Members.

80. Plaintiff and all other Class Members were damaged by CareSource's breach of implied contracts because: (i) they paid monies (directly or through their insurers or CareSource 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
BREACH OF CONTRACTS TO WHICH PLAINTIFF AND CLASS MEMBERS WERE INTENDED THIRD PARTY BENEFICIARIES

81. Plaintiff restates and reallege the preceding allegations above as if fully alleged herein. This claim is pleaded in the alternative to the breach of implied contract claim and all the other claims herein.

82. CareSource had valid contracts with various hospitals, clinics and healthcare providers. It also had contracts with its vendor. A principal purpose of all of those contracts was to securely store, transmit and safeguard the PII/PHI of Plaintiff and Class Members.

83. Upon information and belief, CareSource and each of the contracting hospitals and clinics expressed an intention that Plaintiff and Class Members were intended third party beneficiaries of these agreements.

84. Plaintiff and Class Members are also intended third party beneficiaries of these agreements because recognizing them as such is appropriate to effectuate the intentions of the parties, and the circumstances indicate that CareSource intended to give the beneficiaries the benefit of the promised performance.

85. CareSource breached its agreements with the contracting hospitals and clinics by allowing the data breach to occur, and as otherwise set forth herein.

86. CareSource's breach caused foreseeable and material damages to Plaintiff and Class Members.

COUNT VI
UNJUST ENRICHMENT

87. Plaintiff realleges and incorporate by reference the preceding paragraphs.

88. This claim is pleaded in the alternative to the breach of implied contract claim and intended third party beneficiary claim.

89. In obtaining services or employment from CareSource, Plaintiff and Class Members provided and entrusted their PII and PHI to them.

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

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

92. As a result of CareSource's conduct, Plaintiff and Class Members suffered actual damages.

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

94. CareSource should be compelled to provide for the benefit of Plaintiff and Class Members all unlawful proceeds it received as a result of the conduct and Data Breach alleged herein.

COUNT VII
WEST VIRGINIA CONSUMER CREDIT PROTECTION ACT
W. Va. Code Ann. § 46A-6-101, *et seq.*

95. Plaintiff and the Class repeat and re-allege each allegation as if fully set forth herein.

96. The West Virginia Consumer Credit Protection Act ("WVCCPA") was created to protect West Virginia consumers from deceptive and unfair business practices.

97. CareSource's conduct described herein constitutes unfair methods of competition and unfair or deceptive acts or practices in the conduct of any trade or commerce in West Virginia, making it unlawful under W. Va. Code Ann. §§ 46A-6-104.

98. Plaintiff Cooper and class members suffered ascertainable losses of money or property as the result of the use or employment of a method, act or practice declared unlawful by W. Va. Code Ann. § 46A-6-102(7). Plaintiff and class members acted as reasonable consumers would have acted under the circumstances.

99. Accordingly, pursuant to W. Va. Code § 46A-6-106(a), Plaintiff and class members are entitled to recover their actual damages in the amount to be determined at trial. In addition, given the nature of CareSource's conduct, Plaintiff and West Virginia Subclass Members are entitled to recover statutory damages of $1,000 per violation for the knowing and willful violation of the WVCCPA and attorneys' fees based on the amount of time reasonably expended and equitable relief necessary or proper to protect them from CareSource's unlawful conduct.

PRAYER FOR RELIEF

Plaintiff, individually and on behalf of all other members of the Class, respectfully requests that the Court enter judgment in his favor and against CareSource as follows:

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

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

C. Awarding Plaintiff and the Class equitable, injunctive, and declaratory relief, as may be appropriate. Plaintiff, on behalf of himself and the Class, seeks appropriate injunctive relief designed to prevent CareSource from experiencing yet 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 Plaintiff and the Class pre-judgment and post-judgment interest to the maximum extent allowable;

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

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

JURY TRIAL DEMANDED

Plaintiff demands a trial by jury of all claims in this Class Action Complaint so triable.

Dated: September 4, 2023

Respectfully submitted,

/s/ Terence R. Coates
Terence R. Coates (0085579) – Trial Attorney
Dylan J. Gould (0097954)

MARKOVITS, STOCK & DEMARCO, LLC
119 E. Court Street, Suite 530
Cincinnati, OH 45202
Phone: (513) 651-3700
tcoates@msdlegal.com
dgould@msdlegal.com

Jonathan Shub*
Benjamin F. Johns*
Samantha E. Holbrook*
SHUB & JOHNS LLC
Four Tower Bridge
200 Barr Harbor Drive, Suite 400
Conshohocken, PA 19428
(610) 477-8380
jshub@shublawyers.com
bjohns@shublawyers.com
sholbrook@shublawyers.com

* - pro hac vice forthcoming

Attorneys for Plaintiff