Cause No. 2023CI17950

JASMINE GRACE, individually and on behalf of all others similarly situated, Plaintiff, v. EL CENTRO DEL BARRIO D/B/A CENTROMED, Defendant.	IN THE DISTRICT COURT OF BEXAR COUNTY, TEXAS _____ JUDICIAL DISTRICT CLASS ACTION JURY TRIAL DEMANDED

PLAINTIFF'S ORIGINAL CLASS ACTION PETITION

Plaintiff Jasmine Grace ("Plaintiff"), individually and on behalf of all others similarly situated, brings this Class Action Petition and alleges the following against Defendant El Centro del Barrio d/b/a CentroMed ("CentroMed" or "Defendant"), based upon personal knowledge with respect to Plaintiff and upon information and belief derived from, among other things, investigation of counsel and review of public documents as to all other matters:

NATURE OF THE ACTION

1. This class action arises out of the recent data breach (the "Data Breach") involving CentroMed, which collected and stored certain personally identifiable information ("PII") and/or protected health information ("PHI") of the Plaintiff and approximately 350,000 current and former patients, employees, and

employee and provider spouses / partners / dependents of CentroMed, all of whom have PII/PHI stored on its servers.

2. According to a filing that CentroMed was required to make with the Texas Attorney General, the information compromised in the Data Breach included highly sensitive information including but not limited to: names, addresses, Social Security numbers, "financial information" (such as "account number, credit or debit card number"), health insurance information, and unspecified "medical information." [1]

3. Social Security numbers are particularly valuable to criminals. This information can be sold and traded on the dark web black market. The loss of a Social Security number is particularly troubling because it cannot be easily changed and can be misused in a range of nefarious activities, such as filing fraudulent tax returns to steal tax refund payments, opening new accounts to take out loans, and other forms of identity theft.

4. The Data Breach was a direct result of CentroMed's failure to implement adequate and reasonable cybersecurity procedures and protocols necessary to protect consumers' PII/PHI. Despite discovering the Data Breach on June 12, 2023, CentroMed inexplicably failed to provide notice to impacted patients

[1] https://oag.my.site.com/datasecuritybreachreport/apex/DataSecurityReportsPage (last visited Aug. 23, 2023).

until approximately two months later, on August 11, 2023.[2]

5. CentroMed's notification confirms that its internal investigation "determined that an unauthorized party accessed some of our systems on June 9, 2023" and, while inside the network, "the unauthorized party accessed files that contain information pertaining to CentroMed's current and former patients, employees, and employee and provider spouses / partners / dependents." It went on to state that "[o]ur investigation cannot rule out the possibility that, as a result of this incident, files containing some of your information may have been subject to unauthorized access."

6. Plaintiff and Class Members provided their PII/PHI to CentroMed with the reasonable expectation and on the mutual understanding that CentroMed would comply with its legal obligations to keep such information confidential and secure from unauthorized access.

7. By collecting, using, and deriving a benefit from the PII/PHI of Plaintiff and Class Members, CentroMed assumed legal and equitable duties to those individuals to protect and safeguard that information from unauthorized access and intrusion.

8. Specifically, CentroMed had legal obligations and duties created by

[2] https://www.ksat.com/news/local/2023/08/11/centromed-addresses-data-security-incident-from-june-notifies-affected-individuals/ (last visited Aug. 23, 2023).

HIPAA, contract, industry standards, common law, and representations made to Class Members, to keep Class Members' PII/PHI confidential and to protect it from unauthorized access and disclosure.

9. CentroMed failed to adequately protect Plaintiff's and Class Members' PII/PHI. Cybercriminals targeted and obtained Plaintiff's and Class Members' PII/PHI because of its value in exploiting and stealing the identities of Plaintiff and Class Members. This present and continuing risk to victims of the Data Breach will remain for their respective lifetimes.

10. Had Defendant adequately designed, implemented, and monitored its network and servers, the Data Breach would have been prevented.

11. Had Plaintiff and Class Members known that CentroMed's data security was below industry standards, Plaintiff and Class Members would not have provided their PII/PHI to CentroMed or relied on CentroMed to protect that information.

12. As a result of CentroMed's inadequate data security practices that resulted in the Data Breach, Plaintiff and Class Members are at an imminent risk of identity theft and have suffered numerous actual and concrete injuries and damages, including: (a) invasion of privacy; (b) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft risk; (c) the loss of benefit of the bargain; (d) diminution of value of their PII/PHI; and (e) the

continued risk to their PII/PHI, which remains in the possession of CentroMed, and which is subject to further breaches, so long as CentroMed fails to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' PII/PHI.

13. Plaintiff brings this class action lawsuit on behalf of herself individually as well as all those similarly situated to address CentroMed's inadequate safeguarding of Class Members' PII/PHI that they collected and maintained, and for failing to provide timely and adequate notice to Plaintiff and other Class Members that their information was unsecured and left open to the unauthorized access of any unknown third party.

14. Upon information and belief, CentroMed did not offer or make available to Plaintiff or other victims of the Data Breach any credit monitoring or similar identity theft mitigation product. Instead, CentroMed told people to "review[] the statements they receive from their healthcare providers" and "remain vigilant to the possibility of fraud."

DISCOVERY CONTROL PLAN

15. Due to the complexity of this case, discovery should be conducted pursuant to a discover control plan under Level 3, pursuant to Texas Rule of Civil Procedure 190.4. Plaintiff affirmatively pleads that this suit is not governed by the expedited actions process of Texas Rules of Civil Procedure 169 because Plaintiff

seeks monetary relief in excess of $250,000.00.

PARTIES

Plaintiff

16. Plaintiff Grace is an adult individual and citizen of the State of Texas who resides in San Antonio, Texas. Plaintiff was a patient of CentroMed, which is a healthcare company operating multiple hospitals, healthcare and dental centers. In exchange for receiving medical services, Plaintiff provided Defendant with her PII/PHI as a regular part of Defendant's business operations.

17. Upon information and belief, during the course of her healthcare treatments and as a condition of receiving services from CentroMed, Plaintiff was presented with standard medical forms to complete prior to her treatment that requested her PII/PHI, including Defendant's HIPAA and privacy disclosure forms.

18. Plaintiff greatly values her privacy and the confidentiality of her PII/PHI, especially when submitting information to healthcare providers. Plaintiff takes reasonable steps to secure the confidentiality of her PII/PHI in safe and secure locations and safely destroys sensitive documents.

19. On or around August 11, 2023 an email was sent to Plaintiff from the email address "CentroMed Incident <CMIncident@centromedsa.com>" to notify her of the Data Breach and of the impact to her PII/PHI. As noted above, the email

stated that unauthorized actors gained access to and acquired files on CentroMed network, which included Plaintiff's PII/PHI.

20. Since learning of the Data Breach, Plaintiff has spent significant time in response to the Data Breach, heeding CentroMed's warnings to remain vigilant. She has spent time changing passwords on her accounts and monitoring her credit reports for unauthorized activity, which may take years to discover and detect.

21. Plaintiff plans on taking additional time-consuming but necessary steps to help mitigate the harm caused by the Data Breach, including continually reviewing her credit reports for unauthorized activity.

22. As a result of Defendant's conduct, Plaintiff suffered actual damages including, without limitation, time and expenses related to monitoring her financial accounts for fraudulent activity, facing an increased and imminent risk of fraud and identity theft, the lost value of her personal information, and other economic and non-economic harm. Plaintiff and Class Members will now be forced to expend additional time to review their credit reports and monitor their financial accounts and medical records for fraud or identify theft – particularly since the compromised information may include Social Security numbers.

23. The Data Breach has also caused Plaintiff to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendant has not been

forthright about the cause and full scope of the PII/PHI compromised in the Data Breach.

24. As a result of the Data Breach, Plaintiff anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

25. Plaintiff has a continuing interest in ensuring that her PII/PHI, which, upon information and belief, remains in Defendant's possession, is protected and safeguarded from future breaches.

Defendant

26. Defendant CentroMed, a healthcare organization, is a domestic Texas corporation headquartered at 3750 Commercial Ave, San Antonio, Texas 78221. Defendant may be served through its registered agent, Mr. Ernesto Gomez, at 3750 Commercial Avenue, San Antonio, TX 78221, or wherever it may be found.

JURISDICTION AND VENUE

27. This Court has subject matter jurisdiction over this controversy because the contract between Plaintiff and Defendant was established in Texas. Moreover, the Defendant's failure to adequately safeguard Class Members' data, i.e., the site of Defendant's negligent conduct, occurred in San Antonio, Bexar County, Texas. Plaintiff has been damaged in a sum within the jurisdictional limits of this Court.

28. This Court has personal jurisdiction over Defendant because it is a resident of Texas.

29. Venue is proper in this county under Tex. Civ. Prac. & Rem. Code § 15.002 because a substantial part of the events or omissions giving rise to the claim occurred in this county.

30. Upon information and belief, at least two-thirds of the Class are residents of Texas.

31. Pursuant to Texas Rule of Civil Procedure 47, Plaintiff seeks monetary relief over $1,000,000 for the class.

32. Upon information and belief, Plaintiff's individual damages are less than $75,000.

COMMON FACTUAL ALLEGATIONS

33. El Centro del Barrio was founded in 1971 and, in 2001, began doing business under the name CentroMed.[3]

34. CentroMed operates a network of 23 clinic sites that offer comprehensive quality care by offering Pediatrics, Women's Health, Family

[3] https://centromedsa.com/about-us/ (last visited Aug. 23, 2023).

Practice and Walk-In appointments.[4] It also offers services for dental care, behavioral health, pregnancies, and homeless persons.[5]

35. As noted above, Plaintiff brings this class action against CentroMed for its failure to properly secure and safeguard personally identifiable information, for failing to comply with industry standards to protect and safeguard that information, and for failing to provide timely, accurate, and adequate notice to Plaintiff and other members of the class that such information had been compromised.

Defendant's Unsecure Data Management and Disclosure of Data Breach

36. Plaintiff and Class Members provided their PII/PHI to CentroMed with the reasonable expectation and mutual understanding that CentroMed would comply with its obligations to keep such information confidential and secure from unauthorized access.

37. Plaintiff and Class Members' PII/PHI was provided to CentroMed in conjunction with the type of work Defendant does in providing individual medical and therapeutic needs.

38. In receiving the PII/PHI as part of its services, Defendant assented and undertook legal duties to safeguard and protect the PII/PHI entrusted to them by

[4] https://centromedsa.com/services/ (last visited Aug. 23, 2023).
[5] *Id.*

Plaintiff and Class Members, in compliance with all applicable laws, including HIPAA.

39. Indeed, CentroMed prominently displays a privacy policy which acknowledges that it is legally required to "make sure that your protected health information is kept private." The privacy policy goes on to list several delineated circumstances under which patients' data can be shared with certain third parties (such as for operational uses or in response to a subpoena). Nowhere does it provide that CentroMed can share this sensitive data to unauthorized persons who are able to traverse its IT systems.

40. CentroMed's data security obligations were particularly important given the substantial increase in cyber-attacks and/or data breaches preceding the date it disclosed the incident.

41. CentroMed failed to take appropriate or even the most basic steps to protect the PII/PHI of Plaintiff and other class members from being disclosed.

Plaintiff and the Class Have Suffered Injury as a Result of Defendant's Data Mismanagement

42. As a result of CentroMed's failure to implement and follow even the most basic security procedures, Plaintiff's and Class Members' PII/PHI has been and is now in the hands of unauthorized individuals, which may include thieves, unknown criminals, banks, credit companies, and other potentially hostile individuals. Plaintiff and other Class Members now face an increased risk of identity

theft, particularly due to the dissemination of their Social Security Number, and will consequentially have to spend, and will continue to spend, significant time and money to protect themselves due to CentroMed's Data Breach.

43. Plaintiff and other class members have had their most personal, sensitive and PII/PHI disseminated to the public at large and have experienced and will continue to experience emotional pain and mental anguish and embarrassment.

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

45. Defendant's notification about the breach acknowledged the actual and imminent risk of identity theft as a result of the Data Breach, encouraging them to "remain vigilant" and monitor their financial accounts for many years to mitigate the risk of identity theft.

46. PII/PHI is a valuable property right.[6] The value of PII/PHI as a

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

commodity is measurable.[7] "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."[8] American companies are estimated to have spent over $19 billion on acquiring personal data of consumers in 2018.[9] 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.

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

---

[7] *See* Robert Lowes, *Stolen EHR [Electronic Health Record] Charts Sell for $50 Each on Black Market*, MEDSCAPE (Apr. 28, 2014), http://www.medscape.com/viewarticle/824192 (last visited January 16, 2023).

[8] *Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value*, OECD 4 (Apr. 2, 2013), https://www.oecd-ilibrary.org/science-and-technology/exploring-the-economics-of-personal-data_5k486qtxldmq-en (last visited Aug. 23, 2023).

[9] *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*, INTERACTIVE ADVERTISING BUREAU (Dec. 5, 2018), https://www.iab.com/news/2018-state-of-data-report/ (last visited Aug. 23, 2023).

48. Personal information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[10] Experian reports that a stolen credit or debit card number can sell for $5 to $110 on the dark web.[11] 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.[12] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[13] 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.[14]

---

[10] Anita George, *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends (Oct. 16, 2019), https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last visited Aug. 23, 2023).

[11] Brian Stack, *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian (Dec. 6, 2017), https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last visited Aug. 23, 2023).

[12] Adam Greenberg, *Health insurance credentials fetch high prices in the online black market*, SC MAGAZINE (July 16, 2013), https://www.scmagazine.com/news/breach/health-insurance-credentials-fetch-high-prices-in-the-online-black-market (last visited Aug. 23, 2023)

[13] *In the Dark*, VPNOverview.com, 2019, https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last visited Aug. 23, 2023).

[14] *See Health Care Systems and Medical Devices at Risk for Increased Cyber Intrusions for Financial Gain*, FBI CYBER DIVISION (Apr. 8, 2014),

49. Criminals can use stolen PII/PHI to extort a financial payment by "leveraging details specific to a disease or terminal illness."[15] 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."[16]

50. Consumers place a high value on the privacy of that data. Researchers shed light on how much consumers value their data privacy—and the amount is considerable. Indeed, studies confirm that "when privacy information is made more salient and accessible, some consumers are willing to pay a premium to purchase from privacy protective websites."[17]

51. Given these facts, any company that transacts business with a consumer and then compromises the privacy of consumers' PII/PHI has thus deprived that

---

https://www.illuminweb.com/wp-content/uploads/ill-mo-uploads/103/2418/health-systems-cyber-intrusions.pdf (last visited Aug. 23, 2023).

[15] *See* n.8, *supra*.

[16] *Id.*

[17] Janice Y. Tsai et al., *The Effect of Online Privacy Information on Purchasing Behavior, An Experimental Study*, 22(2) INFORMATION SYSTEMS RESEARCH 254 (June 2011), https://www.jstor.org/stable/23015560?seq=1 (last visited Aug. 23, 2023).

consumer of the full monetary value of the consumer's transaction with the company.

52. Indeed, cyberattacks against the healthcare industry have been common for over ten years with the Federal Bureau of Investigation ("FBI") warning as early as 2011 that cybercriminals were "advancing their abilities to attack a system remotely" and "[o]nce a system is compromised, cyber criminals will use their accesses to obtain PII." The FBI further warned that that "the increasing sophistication of cyber criminals will no doubt lead to an escalation in cybercrime."[18]

53. Cyberattacks have become so notorious that the FBI and U.S. Secret Service have issued a warning to potential targets so they are aware of, and prepared for, a potential attack. As one report explained, "[e]ntities like smaller municipalities and hospitals are attractive to ransomware criminals… because they often have lesser IT defenses and a high incentive to regain access to their data quickly.[19]

[18] Gordon M. Snow, *Statement before the House Financial Services Committee, Subcommittee on Financial Institutions and Consumer Credit*, FBI (Sept. 14, 2011), https://archives.fbi.gov/archives/news/testimony/cyber-security-threats-to-the-financial-sector (last visited Aug. 23, 2023).

[19] Ben Kochman, *FBI, Secret Service Warn of Targeted Ransomware*, LAW360 (Nov. 18, 2019), https://www.law360.com/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware (last visited Aug. 23, 2023).

54. In fact, according to the cybersecurity firm Mimecast, 90% of healthcare organizations experienced cyberattacks in the past year.[20]

55. Defendant was on notice that the FBI has recently been concerned about data security regarding entities that store certain amounts of PHI, as Defendant does. In August 2014, after a cyberattack on Community Health Systems, Inc., the FBI warned companies within the healthcare industry that hackers were targeting them. The warning stated that "[t]he FBI has observed malicious actors targeting healthcare related systems, perhaps for the purpose of obtaining the Protected Healthcare Information (PHI) and/or Personally Identifiable Information (PII)."[21]

56. Plaintiff and members of the Class, as a whole, must immediately devote time, energy, and money to: 1) closely monitor their medical statements, bills, records, and credit and financial accounts; 2) change login and password information on any sensitive account even more frequently than they already do; 3) more carefully screen and scrutinize phone calls, emails, and other communications to ensure that they are not being targeted in a social engineering or spear phishing

[20] *See* Maria Henriquez, *Iowa City Hospital Suffers Phishing Attack,* SECURITY MAGAZINE (Nov. 23, 2020), https://www.securitymagazine.com/articles/93988-iowa-city-hospital-suffers-Phishing-attack (last visited Aug. 23, 2023).

[21] Jim Finkle, *FBI Warns Healthcare Firms that they are Targeted by Hackers*, REUTERS (Aug. 2014), https://www.reuters.com/article/us-cybersecurity-healthcare-fbi/fbi-warns-healthcare-firms-they-are-targeted-by-hackers-idUSKBN0GK24U20140820 (last visited Aug. 23, 2023).

attack; and 4) search for suitable identity theft protection and credit monitoring services, and pay to procure them.

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

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

59. Plaintiff and the Class suffered actual injury from having PII compromised as a result of Defendant's negligent data management and resulting Data Breach including, but not limited to (a) damage to and diminution in the value of their PII/PHI, a form of property that Defendant obtained from Plaintiff; (b) violation of their privacy rights; (c) present and increased risk arising from the identity theft and fraud; (d) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft risk; (e) financial "out of pocket" costs incurred mitigating the materialized risk and imminent threat of identity theft; and (f) invasion of privacy.

60. For the reasons mentioned above, Defendant's conduct, which allowed the Data Breach to occur, caused Plaintiff and members of the Class these significant injuries and harm.

61. Plaintiff brings this class action against Defendant for Defendant's failure to properly secure and safeguard PII/PHI and for failing to provide timely, accurate, and adequate notice to Plaintiff and other class members that their PII/PHI had been compromised.

CLASS ACTION ALLEGATIONS

62. Plaintiff brings this action individually and on behalf of all other persons similarly situated pursuant to Rule 42 of the Texas Rules of Civil Procedure.

63. Plaintiff proposes the following Class definition, subject to amendment as appropriate:

> All persons whose PII/PHI was compromised in the Data Breach occurring in June 2023, including all individuals who Defendant mailed notice to on or around January 12, 2023.

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

65. Plaintiff hereby reserves the right to amend or modify the class definitions with greater specificity or division after having had an opportunity to conduct discovery.

66. Numerosity. The Members of the Classes are so numerous that joinder of all of them is impracticable. As noted above, there are approximately 350,000 Members.

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

a. Whether CentroMed unlawfully used, maintained, lost, or disclosed Plaintiff's and Class Members' PII/PHI;

b. Whether CentroMed failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

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

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

e. Whether CentroMed owed a duty to Class Members to safeguard their

PII/PHI;

f. Whether CentroMed breached their duty to Class Members to safeguard their PII/PHI;

g. Whether computer hackers obtained Class Members' PII/PHI in the Data Breach;

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

i. Whether CentroMed's conduct was negligent;

j. Whether CentroMed's acts, inactions, and practices complained of herein amount to acts of intrusion upon seclusion under the law;

k. Whether CentroMed's acts breaching an implied contract they formed with Plaintiff and the Class Members;

l. Whether CentroMed violated the Federal Trade Commission Act ("FTC Act");

m. Whether CentroMed violated the Health Insurance Portability and Accountability Act ("HIPAA");

n. Whether CentroMed was unjustly enriched to the detriment of Plaintiff and the Class;

o. Whether CentroMed failed to provide notice of the Data Breach in a timely manner; and

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

68. Typicality. Plaintiff's claims are typical of those of other Class Members because Plaintiff's PII/PHI, like that of every other Class Member, was compromised in the Data Breach.

69. Adequacy of Representation. Plaintiff will fairly and adequately represent and protect the interests of the Members of the Class. Plaintiff's Counsel are competent and experienced in litigating class actions, including data privacy litigation of this kind.

70. Predominance. CentroMed has engaged in a common course of conduct toward Plaintiff and Class Members, in that all the Plaintiff's and Class Members' data was stored on the same computer systems and unlawfully accessed in the same way. The common issues arising from CentroMed's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

71. Superiority. A class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most Class Members would likely find that the

cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for CentroMed. In contrast, the conduct of this action as a class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class Member.

72. CentroMed has acted on grounds that apply generally to the Classes as a whole, so that class certification, injunctive relief, and corresponding declaratory relief are appropriate on a class-wide basis.

73. Likewise, particular issues under are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether CentroMed owed a legal duty to Plaintiff and the Classes to exercise due care in collecting, storing, using, and safeguarding their PII/PHI;

b. Whether CentroMed's data security practices were reasonable in light of best practices recommended by data security experts;

c. Whether CentroMed's failure to institute adequate protective security

measures amounted to negligence;

d. Whether CentroMed failed to take commercially reasonable steps to safeguard consumer PII/PHI; and

e. Whether adherence to FTC data security recommendations, and measures recommended by data security experts would have reasonably prevented the Data Breach.

74. Finally, all members of the proposed Classes are readily ascertainable. Defendant has access to Class Members' names and addresses affected by the Data Breach. At least some Class Members have already been preliminarily identified (including plaintiff) and sent notice via email of the Data Breach by Defendant.

CAUSES OF ACTION

COUNT I
NEGLIGENCE

71. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

72. CentroMed owed a duty to Plaintiff and all other Class members to exercise reasonable care in safeguarding and protecting their PII/PHI in their possession, custody, or control.

73. CentroMed 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 secure systems. CentroMed knew, or should have known, of the vast uptick in data breaches in recent years. CentroMed had a duty to protect the PII/PHI of Plaintiff and Class Members.

74. Given the nature of CentroMed's business, the sensitivity and value of the PII/PHI it maintains, and the resources at its disposal, it should have identified the vulnerabilities to its systems and prevented the Data Breach from occurring, which Defendant had a duty to prevent.

75. CentroMed breached these duties by failing to exercise reasonable care in safeguarding and protecting Plaintiff's and Class members' PII/PHI by failing to 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 it—including Plaintiff's and Class members' PII/PHI.

76. It was reasonably foreseeable to CentroMed that its failure to exercise reasonable care in safeguarding and protecting Plaintiff's and Class members' PII/PHI by failing to 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.

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

78. As a result of CentroMed's above-described wrongful actions, inaction, and want of ordinary care that directly and proximately caused the Data Breach, Plaintiff and all other 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 risk of identity theft and medical 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 (vii) actual or attempted fraud.

COUNT II
NEGLIGENCE PER SE

79. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

80. CentroMed's duties arise from, in part due to its storage of certain medical information, *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").

81. CentroMed'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 a business, such as Defendant, of failing to employ reasonable measures to protect and secure PII/PHI.

82. CentroMed's duties further arise from the Health Insurance Portability and Accountability Act of 1996 (HIPAA), 42 U.S.C. § 1302(d), *et seq*.

83. CentroMed is an entity covered under HIPAA, which sets minimum federal standards for privacy and security of PHI.

84. CentroMed violated HIPAA Privacy and Security Rules and Section 5 of the FTCA by failing to use reasonable measures to protect Plaintiff's and all other Class members' PII/PHI and not complying with applicable industry standards. Defendant'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 Plaintiff and the other Class members.

85. CentroMed violations of HIPAA Privacy and Security Rules and Section 5 of the FTCA constitutes negligence per se.

86. 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.

87. 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.

88. It was reasonably foreseeable to CentroMed that its failure to exercise reasonable care in safeguarding and protecting Plaintiff's and Class members' PII/PHI by failing to 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.

89. The injury and harm that Plaintiff and the other Class members suffered was the direct and proximate result of Defendant's violations of HIPAA Privacy and Security Rules and Section 5 of the FTCA. 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 risk of identity theft and medical 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) actual or attempted fraud.

COUNT III
BREACH OF FIDUCIARY DUTY

90. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

91. Plaintiff and Class members either directly or indirectly gave Defendant their PII/PHI in confidence, believing that CentroMed – a healthcare service provider – would protect that information. Plaintiff and Class members would not have provided Defendant with this information had they known it would not be adequately protected. Defendant's acceptance and storage of Plaintiff's and Class members' PII/PHI created a fiduciary relationship between Defendant and Plaintiff and Class Members. In light of this relationship, Defendant must act primarily for the benefit of its patients, which includes safeguarding and protecting Plaintiff's and Class Members' PII/PHI.

92. Defendant has a fiduciary duty with respect to the PII/PHI entrusted to it 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 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 the PII/PHI of Plaintiff and Class Members it collected.

93. As a direct and proximate result of CentroMed's breaches of its fiduciary duties, Plaintiff and Class members have suffered and will suffer injury, including, but not limited to: (i) a substantial increase in the likelihood 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 effort attempting to mitigate the actual and future consequences of the Data Breach; (v) the continued risk to their PII/PHI which remains in Defendant'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) actual or attempted fraud.

COUNT IV
UNJUST ENRICHMENT

94. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein. This claim is pled in the alternative to the implied contract claim.

95. Plaintiff and Class Members conferred a monetary benefit upon Defendant in the form of monies paid for healthcare services or other services.

96. Defendant accepted or had knowledge of the benefits conferred upon it by Plaintiff and Class Members. Defendant also benefitted from the receipt of Plaintiff's and Class Members' PII/PHI.

97. As a result of Defendant's conduct, Plaintiff and Class Members suffered actual damages in an amount equal to the difference in value between their payments made with reasonable data privacy and security practices and procedures that Plaintiff and Class Members paid for, and those payments without reasonable data privacy and security practices and procedures that they received.

98. Defendant should not be permitted to retain the money belonging to Plaintiff and Class Members because Defendant failed to adequately implement the data privacy and security procedures for itself that Plaintiff and Class Members paid for and that were otherwise mandated by federal, state, and local laws. and industry standards.

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

COUNT V
BREACH OF IMPLIED CONTRACT

100. Plaintiff realleges and incorporates by reference all allegations of the preceding factual allegations as though fully set forth herein.

101. Defendant required Plaintiff and Class Members to provide, or authorize the transfer of, their PII/PHI in order for Defendant to provide services. In exchange, Defendant entered into implied contracts with Plaintiff and Class Members in which Defendant agreed to comply with its statutory and common law duties to protect Plaintiff's and Class Members' PII/PHI and to timely notify them in the event of a data breach.

102. Plaintiff and Class Members would not have provided their PII/PHI to Defendant had they known that Defendant would not safeguard their PII/PHI, as promised, or provide timely notice of a data breach.

103. Plaintiff and Class Members fully performed their obligations under their implied contracts with Defendant.

104. Defendant breached the implied contracts by failing to safeguard Plaintiff's and Class Members' PII/PHI and by failing to provide them with timely and accurate notice of the Data Breach.

105. The losses and damages Plaintiff and Class Members sustained (as described above) were the direct and proximate result of Defendant's breach of its implied contracts with Plaintiff and Class Members.

STATEMENT REGARDING USE OF DOCUMENTS

106. Pursuant to Texas Rule of Civil Procedure 193.7, Plaintiff hereby gives notice that any and all documents produced by Defendant in this matter may be used against Defendant at any pre-trial proceeding or at trial without the necessity of authenticating the produced documents.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of the Classes, pray for judgment as follows:

a. For an Order certifying this action as a class action and appointing Plaintiff and her counsel to represent the Class and Subclass;

b. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and Class Members' PII/PHI;

c. For equitable relief compelling Defendant to utilize appropriate methods and policies with respect to consumer data collection, storage, and safety, and to disclose with specificity the type of PII/PHI compromised during the Data Breach;

d. For an order requiring Defendant to pay for credit monitoring services for Plaintiff and the Class of a duration to be determined at trial;

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

f. For an award of punitive damages, as allowable by law;

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

h. Pre- and post-judgment interest on any amounts awarded; and

i. Such other and further relief as this court may deem just and proper.

JURY TRIAL DEMANDED

Plaintiff demands a trial by jury on all claims so triable.

Dated: August 23, 2023

Respectfully Submitted By:

By: */s/ Ketan U. Kharod*

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

**Pro Hac Vice Forthcoming*

Ketan U. Kharod
Texas Bar No. 24027105
GUERRERO & WHITTLE, PLLC
2630 Exposition Blvd., Suite 102
Austin, TX 78703
Telephone: (512) 605-2300
Fax: (512) 222-5280
ketan@gwjustice.com

Attorneys for Plaintiff and the Proposed Class

Automated Certificate of eService

This automated certificate of service was created by the efiling system. The filer served this document via email generated by the efiling system on the date and to the persons listed below. The rules governing certificates of service have not changed. Filers must still provide a certificate of service that complies with all applicable rules.

Ketan Kharod on behalf of Ketan Kharod
Bar No. 24027105
ketan@gwjustice.com
Envelope ID: 78859414
Filing Code Description: Petition
Filing Description:
Status as of 8/24/2023 8:39 AM CST

Associated Case Party: Jasmine Grace

Name	BarNumber	Email	TimestampSubmitted	Status
Ketan UKharod		ketan@gwjustice.com	8/23/2023 11:02:07 PM	SENT
Gaby Deras		gaby@gwjustice.com	8/23/2023 11:02:07 PM	SENT
Benjamin Johns		bjohns@shublawyers.com	8/23/2023 11:02:07 PM	SENT
Damian Gomez		dgomez@shublawyers.com	8/23/2023 11:02:07 PM	SENT