Filed
Submitted 12/15/2022 8:00 AM
Stephnie Menke
District Clerk Potter County, Texas
Envelope No. 71027275
Filed: 12/15/2022 9:57 AM
By: PB

CAUSE NO. 111219-D-CV

DENELI SHARBER, SHANNA BYERS, LYLE SCHAFER, and JENNIFER HART, individually and on behalf of all others similarly situated, Plaintiffs, v. FMC SERVICES, LLC, d/b/a Family Medicine Centers, Defendant.	IN THE DISTRICT COURT OF POTTER COUNTY, TEXAS 320th JUDICIAL DISTRICT CLASS ACTION JURY TRIAL DEMANDED

CONSOLIDATED CLASS ACTION PETITION

Plaintiffs Deneli Sharber, Shanna Byers, Lyle Schafer, and Jennifer Hart (formerly Holman), ("Plaintiffs"), individually and on behalf of all others similarly situated (collectively, "Class members"), by and through their undersigned attorneys, bring this Consolidated Class Action Petition against Defendant FMC Services, LLC, d/b/a Family Medicine Centers ("FMC"), and complain and allege upon personal knowledge as to themselves and information and belief as to all other matters.

INTRODUCTION

1. Plaintiffs bring this class action against FMC for its failure to secure and safeguard the personally identifiable information ("PII") and personal health information ("PHI") of approximately 233,948 individuals, including Plaintiffs. The data reportedly exposed in the breach includes the most sensitive types of data that cybercriminals seek in order to commit fraud and identity theft. According to FMC, information disclosed in the breach includes names, mailing addresses, dates of birth, Social Security numbers, and protected health information.

2. FMC is a healthcare company with its principal place of business in Amarillo, Texas. The company has four clinics at which it provides standard medical services as well as urgent care clinics called CareXpress.

3. On or about July 26, 2022, FMC determined that unauthorized individuals had gained access to its network systems, and accessed the PII/PHI of Plaintiffs and Class members (the "Data Breach").

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

5. As a result of FMC's inadequate security and breach of its duties and obligations, the Data Breach occurred, and Plaintiffs' and Class members' PII/PHI was accessed and disclosed. This action seeks to remedy these failings and their consequences. Plaintiffs bring this action on behalf of themselves and all persons whose PII/PHI was exposed as a result of the Data Breach, which FMC learned of on or about July 26, 2022, and first publicly acknowledged in September of 2022.

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

PARTIES

7. Plaintiff Deneli Sharber is a Texas resident. The last three digits of her driver's license number are 491. The last three digits of her Social Security number are 636. Plaintiff Sharber has obtained services from FMC. Plaintiff Sharber received a letter from FMC notifying her that her PII/PHI was among the information accessed by cybercriminals in the Data Breach Had Plaintiff Sharber known that FMC would not adequately protect her and Class members' PII/PHI, she would not have received services from FMC and would not have provided her PII/PHI to FMC. Plaintiff Sharber monitors her financial accounts for about 20 minutes per week. Additionally, Plaintiff Sharber has started receiving 10-15 spam emails a day written in foreign language and also ones concerning her private health information. She thinks that they are related to the Data Breach since she has only received those since about the time of the breach or after.

8. Plaintiff Shanna Byers is a Texas resident. The last three digits of her driver's license number are 348. The last three digits of her Social Security number are 476. Plaintiff Byers has obtained services from FMC. Plaintiff Byers received a letter from FMC notifying her that her PII/PHI was among the information accessed by cybercriminals in the Data Breach. Had Plaintiff Byers known that FMC would not adequately protect her and Class members' PII/PHI, she would not have received services from FMC and would not have provided her PII/PHI to FMC. Plaintiff Byers monitors her financial accounts for about 20 minutes per week. Plaintiff Byers has noticed a significant increase in spam calls and emails since the Data Breach occurred.

9. Plaintiff Lyle Schafer is a Texas resident. The last three digits of his driver's license number are 664. The last three digits of his Social Security number are 677. Plaintiff Schafer has obtained services from FMC. Plaintiff Schafer received a letter from FMC notifying him that his PII/PHI was among the information accessed by cybercriminals in the Data Breach. Had Plaintiff

Schafer known that FMC would not adequately protect his and Class members' PII/PHI, he would not have received services from FMC and would not have provided his PII/PHI to FMC. Around the time Plaintiff Schafer received the letter from FMC, he also received written notice that one of his credit cards had been cancelled due to fraudulent charges having been placed on it. He subsequently confirmed that he had used that card at FMC, and filed a police report on the incidents. Plaintiff Schafer is confident that the fraudulent charges are attributable to the FMC Data Breach because he long ago cancelled cards that were compromised in other data breaches. Plaintiff Schafer has also experienced increased spam in both his email and text messages since the Data Breach.

10. Plaintiff Jennifer Hart (formerly Holman) is a Texas resident. The last three digits of her driver's license number are 663. The last three digits of her Social Security number are 913. Plaintiff Hart has obtained services from FMC. Plaintiff Hart received a letter from FMC notifying her that her PII/PHI was among the information accessed by cybercriminals in the Data Breach. Had Plaintiff Hart known that FMC would not adequately protect her and Class members' PII/PHI, she would not have received services from FMC and would not have provided her PII/PHI to FMC. On October 3, 2022, Plaintiff Hart was notified by Norton 360 Identity Theft Protection that her personal information was placed and used by an unknown individual on the dark web. On October 6, 2022, an unknown individual stole Plaintiff Hart's Capital One Credit Card information and attempted to make fraudulent purchases with her card. This drove her credit card over its available credit limit and negatively affected her credit score. In addition, she experienced a substantial number of spam emails, text, messages, and phone calls following the Data Breach, which Plaintiff Hart believes is related to her private information being placed in the hands of an illicit actor.

11. Defendant FMC Services, LLC, d/b/a Family Medicine Centers is a limited liability company formed in Texas and has its principal place of business at 2501 Lakeview Drive, Amarillo, Texas 79109.

JURSDICTION AND VENUE

12. The Court has subject matter jurisdiction over Plaintiffs' claims pursuant to Article V § 8 of the Texas Constitution because no other court has exclusive or original jurisdiction over this matter.

13. This Court has personal jurisdiction over FMC because FMC was formed in Texas and has its principal place of business in Amarillo, Texas.

14. Venue is proper in this county pursuant to Texas Civil Practice and Remedies Code Section 15.002(3) because FMC's principal place of business is located in this county.

15. While the damages to be awarded lie within the sound discretion of the fact finder based on the evidence as presented, Plaintiffs recognize the pleading requirements of Rule 47 of the Texas Rules of Civil Procedure. Accordingly, Plaintiffs seek monetary relief over $1,000,000, which exceeds this Court's minimum jurisdictional requirements.

DISCOVERY CONTROL PLAN LEVEL

16. Pursuant to Texas Rule of Civil Procedure 190, Plaintiffs state that discovery in this matter is intended to be conducted under Level III, as specified by Tex. R. Civ. P. 190.4.

FACTUAL ALLEGATIONS

Overview of FMC

17. FMC has locations in Amarillo and Canyon, Texas. The company employs approximately 75 health care providers across all of its clinics.[1]

18. In the regular course of its business, FMC collects and maintains the PII/PHI of patients, former patients, and other persons to whom it is currently providing or previously provided health-related or other services.

19. FMC requires patients to provide personal information before it provides them services. That information includes demographic information, health insurance information, and Social Security numbers.

20. Plaintiffs and Class members are, or were, patients of FMC or received health-related or other services from FMC, and entrusted FMC with their PII/PHI.

21. FMC acknowledges its responsibility to protect Plaintiffs' and other Class members' PII/PHI. On its website, FMC states that its privacy policy "is designed to be compliant with applicable state and Federal law."[2] FMC provides its privacy policy to its patients when they receive services at a clinic and requires new patients to sign a form acknowledging that they received a copy of the privacy policy.[3] Despite this acknowledgment that it must protect its patients' PII/PHI, FMC fails and has failed to do so.

---

[1] *About Us*, FAMILY MEDICINE CENTERS, https://www.fmcclinics.com/about-us (last visited Dec. 9, 2022).
[2] *Id*.
[3] *See*, *e.g.*, https://www.fmcclinics.com/_files/ugd/7092fc_3404ce1a7cad44d28bf543de75cc0814.pdf (Coulter clinic); https://www.fmcclinics.com/_files/ugd/7092fc_fc3d68ecf375469d9d9d9a637977f5a0.pdf (34th and Coulter clinic) (last visited Dec. 9, 2022).

The Data Breach

22. On or about July 26, 2022, FMC discovered that unauthorized users had gained access to its network systems.

23. On August 21, 2022, the Vice Society, which the federal government describes as an "intrusion, exfiltration, and extortion hacking group,"[4] published over 272,000 files that it claimed to have taken from FMC and an affiliated health care provider, BSA Hospice.[5] FMC did not respond to questions regarding the files, and did not notify authorities or victims about the Data Breach until over a month later.[6] FMC's notice does not warn those affected that their information was released by cybercriminals.

24. On or about September 23, 2022, FMC reported the Data Breach to state attorneys general and the United States Department of Health and Human Services and posted a notice of the Data Breach on its website.[7]

25. FMC reports to the affected individuals that the information involved in the Data Breach includes an individual's "name, mailing address, date of birth, Social Security Number, and/or protected health information may have been exposed as a result of the attack."[8]

---

[4] *See Alert (AA22-249A) #StopRansomware: Vice Society*, CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY (Sept. 6, 2022), https://www.cisa.gov/uscert/ncas/alerts/aa22-249a.
[5] *See A Confusing Data Dump from Vice Society*, DATABREACHES.NET (Aug. 26, 2022), https://www.databreaches.net/a-confusing-data-dump-from-vice-society/.
[6] *See Why Won't They Tell You That Your Data Was Leaked? Why Doesn't the Government Make Them Tell You?*, DATABREACHES.NET (Oct. 3, 2022), https://www.databreaches.net/why-wont-they-tell-you-that-your-data-were-leaked-why-doesnt-the-government-make-them-tell-you/.
[7] *See* Notice of Data Incident, FAMILY MEDICINE CENTERS, https://www.fmcclinics.com/notice-of-data-incident (last visited Dec. 9, 2022).
[8] *Id*.

26. FMC began to notify its patients of these alleged facts via the Notice of Data Incident on its website and the letters that FMC provided to impacted persons. FMC reported to the United States Department of Health and Human Services that the breach affected 233,948 persons.[9]

FMC Knew That Criminals Target PII/PHI

27. At all relevant times, FMC knew, or should have known, its patients', Plaintiffs', and all other Class members' PII/PHI was a target for malicious actors. Despite such knowledge, FMC failed to implement and maintain reasonable and appropriate data privacy and security measures to protect Plaintiffs' and Class members' PII/PHI from cyber-attacks that FMC should have anticipated and guarded against.

28. Cyber criminals seek out PHI at a greater rate than other sources of personal information. In a 2022 report, the healthcare compliance company Protenus found that there were 905 medical data breaches in 2021 with over 50 million patient records exposed.[10] This is an increase from the 758 medical data breaches which exposed approximately 40 million records that Protenus compiled in 2020.[11]

29. PII/PHI is a valuable property right.[12] The value of PII/PHI as a commodity is measurable.[13] "Firms are now able to attain significant market valuations by employing business

---

[9] *See* https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (last visited Dec. 9, 2022).
[10] PROTENUS, *2022 Breach Barometer*, PROTENUS.COM, https://www.protenus.com/breach-barometer-report (last visited Dec. 9, 2022).
[11] *Id*.
[12] *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 . . . .").
[13] *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.

models predicated on the successful use of personal data within the existing legal and regulatory frameworks."[14] American companies are estimated to have spent over $19 billion on acquiring personal data of consumers in 2018.[15] 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.

30. 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, SSNs, PII/PHI, and other sensitive information directly on various Internet websites making the information publicly available. This information from various breaches, including the information exposed in the Data Breach, can be aggregated and become more valuable to thieves and more damaging to victims.

31. PHI is particularly valuable and has been referred to as a "treasure trove for criminals."[16] A cybercriminal who steals a person's PHI can end up with as many as "seven to ten personal identifying characteristics of an individual."[17] A study by Experian found that the "average total cost" of medical identity theft is "about $20,000" per incident, and that a majority of victims of medical identity theft were forced to pay out-of-pocket costs for healthcare they did not receive in order to restore coverage.[18]

---

[14] *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.

[15] *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/.

[16] *See* Andrew Steger, *What Happens to Stolen Healthcare Data?*, HEALTHTECH MAGAZINE (Oct. 30, 2019), https://healthtechmagazine.net/article/2019/10/what-happens-stolen-healthcare-data-perfcon (quoting Tom Kellermann, Chief Cybersecurity Officer, Carbon Black, stating "Health information is a treasure trove for criminals.").

[17] *Id.*

[18] Elinor Mills, *Study: Medical identity theft is costly for victims*, CNET (Mar. 3, 2010, 5:00 A.M.), https://www.cnet.com/news/study-medical-identity-theft-is-costly-for-victims.

32. 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.[19] 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.[20]

33. Criminals can use stolen PII/PHI to extort a financial payment by "leveraging details specific to a disease or terminal illness."[21] 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."[22]

34. 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."[23]

---

[19] SC Staff, *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.

[20] *See Health Care Systems and Medical Devices at Risk for Increased Cyber Intrusions for Financial Gain*, FBI CYBER DIVISION (Apr. 8, 2014), https://www.illuminweb.com/wp-content/uploads/ill-mo-uploads/103/2418/health-systems-cyber-intrusions.pdf.

[21] *See What Happens to Stolen Healthcare Data*, n.16, *supra*.

[22] *Id.*

[23] 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.

35. 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

36. Theft of PII/PHI is serious. The Federal Trade Commission ("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.[24]

37. Identity thieves use personal information for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.[25] According to Experian, one of the largest credit reporting companies in the world, "[t]he research shows that personal information is valuable to identity thieves, and if they can get access to it, they will use it" to among other things: open a new credit card or loan, change a billing address so the victim no longer receives bills, open new utilities, obtain a mobile phone, open a bank account and write bad checks, use a debit card number to withdraw funds, obtain a new driver's license or ID, or use the victim's information in the event of arrest or court action.[26]

---

[24] *See What to Know About Identity Theft*, FEDERAL TRADE COMMISSION CONSUMER ADVICE, https://www.consumer.ftc.gov/articles/what-know-about-identity-theft (last visited Dec. 9, 2022).

[25] 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).

[26] *See* Susan Henson, *What Can Identity Thieves Do with Your Personal Information and How Can You Protect Yourself?*, EXPERIAN (Sept. 1, 2017), https://www.experian.com/blogs/ask-experian/what-can-identity-thieves-do-with-your-personal-information-and-how-can-you-protect-yourself/.

38. 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.[27]

39. 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.[28]

40. 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 her SSN, and a new SSN will not be provided until after the harm has already been suffered by the victim.

41. 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 haven't gotten a credit freeze yet, you're easy pickings."[29]

---

[27] *See Warning Signs of Identity Theft*, FEDERAL TRADE COMMISSION, https://www.identitytheft.gov/Warning-Signs-of-Identity-Theft (last visited Dec. 9, 2022).
[28] *2021 Consumer Aftermath Report: How Identity Crimes Impact Victims, Their Families, Friends And Workplaces*, IDENTITY THEFT RESOURCE CENTER, https://www.idtheftcenter.org/identity-theft-aftermath-study/ (last visited Dec. 9, 2022).
[29] Patrick Lucas Austin, *'It Is Absurd.' Data Breaches Show it's Time to Rethink How We Use Social Security Numbers, Experts Say*, TIME (Aug. 5, 2019, 3:39 P.M.), https://time.com/5643643/capital-one-equifax-data-breach-social-security/.

42. 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."[30] It "is also more difficult to detect, taking almost twice as long as normal identity theft."[31] In warning consumers on the dangers of medical identity theft, the FTC states that an identity thief may use PII/PHI "to see a doctor, get prescription drugs, buy medical devices, submit claims with your insurance provider, or get other medical care." [32] 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. It could also hurt your credit."[33]

43. 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 not 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

[30] Pam Dixon and John Emerson, *Report: The Geography of Medical Identity Theft*, WORLD PRIVACY FORUM 6 (Dec. 12, 2017), https://www.worldprivacyforum.org/2017/12/new-report-the-geography-of-medical-identity-theft/.
[31] *See Health Care Systems and Medical Devices at Risk*…, n.20, *supra*.
[32] *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 visited Dec. 9, 2022).
[33] *Id*.

imposter; victims have been denied jobs due to incorrect information placed in their health files due to the crime.

- As a result of improper or fraudulent medical debt reporting, victims may not qualify for mortgage or other loans and may experience other financial impacts.
- Phantom medical debt collection based on medical billing or other identity information.
- Sales of medical debt arising from identity theft can perpetuate a victim's debt collection and credit problems, through no fault of their own.[34]

44. 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 and it takes some individuals up to three years to learn that information.[35]

45. It is within this context that Plaintiffs and all other Class members must now live with the knowledge that their PII/PHI is forever in cyberspace and was taken by people willing to use the information for any number of improper purposes and scams, including making the information available for sale on the black-market.

Damages Sustained by Plaintiffs and the Other Class Members

46. Plaintiffs sand all other Class members have suffered injury and damages, including, but not limited to: (i) a substantially increased risk of identity theft and medical identity theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (ii) improper disclosure of their PII/PHI; (iii) breach of the confidentiality of their PII/PHI; (iv) deprivation of the value of their PII/PHI, for which there is a well-established national and international market; (v) lost time and money incurred to mitigate and remediate the

[34] *See The Geography of Medical Identity Theft*, n.30, *supra*.
[35] John W. Coffey, *Difficulties in Determining Data Breach Impacts*, 17 JOURNAL OF SYSTEMICS, CYBERNETICS AND INFORMATICS 9 (2019), http://www.iiisci.org/journal/pdv/sci/pdfs/IP069LL19.pdf.

effects of the Data Breach, including the increased risks of identity theft and medical identity theft they face and will continue to face; and (vi) overpayment for the services that were received without adequate data security.

CLASS ALLEGATIONS

47. This action is brought and may be properly maintained as a class action pursuant to Rule 42 of the Texas Rules of Civil Procedure.

48. Plaintiffs bring this action on behalf of themselves 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.

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

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

51. The members in the Class are so numerous that joinder of all Class members in a single proceeding would be impracticable. FMC reported to the United States Department of Health and Human Services that the breach affected 233,948 persons.

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

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

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

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

E. Whether Plaintiffs and all other members of the Class are entitled to damages and the measure of such damages and relief.

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

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

55. Plaintiffs will fairly and adequately protect the interests of the Class members. Plaintiffs are adequate representatives of the Class in that Plaintiffs have no interests adverse to,

or that conflict with, the Class Plaintiffs seek to represent. Plaintiffs have retained counsel with substantial experience and success in the prosecution of complex consumer protection class actions of this nature.

56. A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. The damages and other financial detriment suffered by Plaintiffs and all other Class members are relatively small compared to the burden and expense that would be required to individually litigate their claims against FMC, so it would be impracticable for Class members to individually seek redress from FMC'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

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

58. FMC owed a duty to Plaintiffs and all other Class members to exercise reasonable care in safeguarding and protecting their PII/PHI in its possession, custody, or control.

59. FMC knew the risks of collecting and storing Plaintiffs' and all other Class members' PII/PHI and the importance of maintaining secure systems. FMC knew of the many data breaches that targeted healthcare providers in recent years.

60. Given the nature of FMC's business, the sensitivity and value of the PII/PHI it maintains, and the resources at its disposal, FMC should have identified the vulnerabilities to their systems and prevented the Data Breach from occurring.

61. FMC breached these duties by failing to exercise reasonable care in safeguarding and protecting Plaintiffs' 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 Plaintiffs' and Class members' PII/PHI.

62. It was reasonably foreseeable to FMC that its failure to exercise reasonable care in safeguarding and protecting Plaintiffs' 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 Plaintiffs' and Class members' PII/PHI to unauthorized individuals.

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

64. As a result of FMC's above-described wrongful actions, inaction, and want of ordinary care that directly and proximately caused the Data Breach, Plaintiffs 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 identity theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (ii) improper disclosure of their PII/PHI; (iii) breach of the confidentiality of their PII/PHI; (iv) deprivation of the value of their PII/PHI, for which there is a

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

COUNT II
NEGLIGENCE PER SE

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

66. FMC'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").

67. FMC'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 FMC, of failing to employ reasonable measures to protect and secure PII/PHI.

68. FMC violated HIPAA Privacy and Security Rules and Section 5 of the FTCA by failing to use reasonable measures to protect Plaintiffs' and all other Class members' PII/PHI and not complying with applicable industry standards. FMC's conduct was particularly unreasonable given the nature and amount of PII/PHI it obtains and stores, and the foreseeable consequences of a data breach involving PII/PHI including, specifically, the substantial damages that would result to Plaintiffs and the other Class members.

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

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

71. 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.

72. It was reasonably foreseeable to FMC that its failure to exercise reasonable care in safeguarding and protecting Plaintiffs' 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 Plaintiffs' and Class members' PII/PHI to unauthorized individuals.

73. The injury and harm that Plaintiffs and the other Class members suffered was the direct and proximate result of FMC'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 identity theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (ii) improper disclosure of their PII/PHI; (iii) breach of the confidentiality of their PII/PHI; (iv) deprivation of the value of their PII/PHI, for which there is a well-established national and international market; (v) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of medical identity theft they face and will continue to face; and (vi) overpayment for the services that were received without adequate data security.

COUNT III
BREACH OF FIDUCIARY DUTY

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

75. Plaintiffs and Class members gave FMC their PII/PHI in confidence, believing that FMC would protect that information. Plaintiffs and Class members would not have provided FMC with this information had they known it would not be adequately protected. FMC's acceptance and storage of Plaintiffs' and Class members' PII/PHI created a fiduciary relationship between FMC and Plaintiffs and Class members. In light of this relationship, FMC must act primarily for the benefit of its patients and former patients, which includes safeguarding and protecting Plaintiffs' and Class Members' PII/PHI.

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

77. As a direct and proximate result of FMC's breaches of its fiduciary duties, Plaintiffs 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 FMC's possession; (vi) future costs in terms of time, effort, and money that will be required to prevent, detect, and repair the impact of the PII/PHI

compromised as a result of the Data Breach; and (vii) overpayment for the services that were received without adequate data security.

COUNT IV
BREACH OF IMPLIED CONTRACT

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

79. In connection with receiving medical services, Plaintiffs and all other Class members entered into implied contracts with FMC.

80. Pursuant to these implied contracts, Plaintiffs and Class members paid money to FMC, whether directly or through their insurers, and provided FMC with their PII/PHI. In exchange, FMC agreed to, among other things, and Plaintiffs understood that FMC would: (1) provide medical services to Plaintiffs and Class member; (2) take reasonable measures to protect the security and confidentiality of Plaintiffs' and Class members' PII/PHI; and (3) protect Plaintiffs' and Class members PII/PHI in compliance with federal and state laws and regulations and industry standards.

81. The protection of PII/PHI was a material term of the implied contracts between Plaintiffs and Class members, on the one hand, and FMC, on the other hand. Indeed, as set forth *supra*, FMC recognized its duty to provide adequate data security and ensure the privacy of its patients' PII/PHI with its practice of providing patients with a privacy policy. Had Plaintiffs and Class members known that FMC would not adequately protect its patients' and former patients' PII/PHI, they would not have received services from FMC.

82. Plaintiffs and Class members performed their obligations under the implied contract when they provided FMC with their PII/PHI and paid—directly or through their insurers—for health care services from FMC.

83. FMC breached its obligations under its implied contracts with Plaintiffs and Class members in failing to implement and maintain reasonable security measures to protect and secure their PII/PHI and in failing to implement and maintain security protocols and procedures to protect Plaintiffs' and Class members' PII/PHI in a manner that complies with applicable laws, regulations, and industry standards.

84. FMC's breach of its obligations of its implied contracts with Plaintiffs and Class members directly resulted in the Data Breach and the injuries that Plaintiffs and all other Class members have suffered from the Data Breach.

85. Plaintiffs and all other Class members were damaged by FMC's breach of implied contracts because: (i) they paid—directly or through their insurers—for data security protection they did not receive; (ii) they face a substantially increased 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) 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) overpayment for the services that were received without adequate data security.

COUNT V
UNJUST ENRICHMENT

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

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

88. Plaintiffs and Class members conferred a monetary benefit upon FMC in the form of monies paid for healthcare services or other services.

89. FMC accepted or had knowledge of the benefits conferred upon it by Plaintiffs and Class Members. FMC also benefitted from the receipt of Plaintiffs' and Class members' PHI, as this was used to facilitate payment.

90. As a result of FMC's conduct, Plaintiffs 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 Plaintiffs and Class members paid for, and those payments without reasonable data privacy and security practices and procedures that they received.

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

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

PRAYER FOR RELIEF

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

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

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

C. Awarding Plaintiffs and the Class equitable, injunctive, and declaratory relief, as may be appropriate. Plaintiffs, on behalf of themselves and the Class, seek appropriate injunctive relief designed to prevent FMC from experiencing another data breach by adopting and implementing best data security practices to safeguard PII/PHI and to provide or extend credit monitoring services and similar services to protect against all types of identity theft and medical identity theft;

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

E. Awarding Plaintiffs and the Class reasonable attorneys' fees, costs, and expenses, pursuant to Texas Rule of Civil Procedure 42, as allowable; and

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

JURY TRIAL DEMANDED

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

Dated: December 14, 2022

Respectfully submitted,

/s/ J. Daren Brown

J. Daren Brown
STOCKARD, JOHNSTON, BROWN, NETARDUS & DOYLE, P.C.
TSBN: 24036271
1030 N. Western Street
Amarillo, Texas 79106
Telephone: (806) 372-2202
Facsimile: (806) 379-7799
dbrown@sjblawfirm.com

Interim Liaison Counsel

Ben Barnow (pro hac vice)
Anthony L. Parkhill (pro hac vice)
Riley W. Prince (pro hac vice)
BARNOW AND ASSOCIATES, P.C.
205 West Randolph Street, Ste. 1630
Chicago, IL 60606
Tel: 312-621-2000
Fax: 312-641-5504
b.barnow@barnowlaw.com
aparkhill@barnowlaw.com
rprince@barnowlaw.com

Gary E. Mason*
Danielle Perry*
Lisa A. White*
MASON LLP
5301 Wisconsin Avenue, NW
Suite 305
Washington, DC 20016
Tel: (202) 429-2290
gmason@masonllp.com
dperry@masonllp.com
lwhite@masonllp.com

Interim Co-Lead Counsel

John G. Turner III (TX# 203020550)
Robert R. Bell III (TX# 00787062)
BAILEY & GLASSER LLP
P.O. Box 1089
Hewin, TX 76643
(304) 345-6555
jturner@baileyglasser.com
rbell@baileyglasser.com

Bart D. Cohen*
BAILEY & GLASSER LLP
1622 Locust Street
Philadelphia, PA 19103
(215) 274-9420
bcohen@baileyglasser.com

Brian C. Gudmundson*

Jason P. Johnston*
Michael J. Laird*
Rachel K. Tack*
ZIMMERMAN REED LLP
1100 IDS Center
80 South 8th Street
Minneapolis, MN 55402
Telephone: (612) 341-0400
Facsimile: (612) 341-0844
brian.gudmundson@zimmreed.com
jason.johnston@zimmreed.com
michael.laird@zimmreed.com
rachel.tack@zimmreed.com

Christopher D. Jennings*
Nathan I. Reiter III*
THE JOHNSON FIRM
610 President Clinton Ave., Suite 300
Little Rock, AR 72201
Tel: (501) 372-1300
chris@yourattorney.com
nathan@yourattorney.com

**pro hac vice* to be submitted

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.

Courtney Neely on behalf of John Brown
Bar No. 24036271
cneely@sjblawfirm.com
Envelope ID: 71027275
Status as of 12/15/2022 9:57 AM CST

Associated Case Party: Deneli Sharber

Name	BarNumber	Email	TimestampSubmitted	Status
William BFederman		wbf@federmanlaw.com	12/14/2022 5:05:16 PM	SENT
Administrative Administrative		law@federmanlaw.com	12/14/2022 5:05:16 PM	SENT
Gary E.Mason		gmason@masonllp.com	12/14/2022 5:05:16 PM	SENT
Taylor Heath		theath@masonllp.com	12/14/2022 5:05:16 PM	SENT
Jenni Suhr		jsuhr@masonllp.com	12/14/2022 5:05:16 PM	SENT
Danielle L.Perry		dperry@masonllp.com	12/14/2022 5:05:16 PM	SENT
Lisa A.White		lwhite@masonllp.com	12/14/2022 5:05:16 PM	SENT

Associated Case Party: Jennifer Holman

Name	BarNumber	Email	TimestampSubmitted	Status
Ryan LThompson		rthompson@triallawyers.com	12/14/2022 5:05:16 PM	SENT
Meganne Feula		mfeula@triallawyers.com	12/14/2022 5:05:16 PM	SENT
Rachel Tack		rachel.tack@zimmreed.com	12/14/2022 5:05:16 PM	SENT

Case Contacts

Name	BarNumber	Email	TimestampSubmitted	Status
Courtney Neely		cneely@sjblawfirm.com	12/14/2022 5:05:16 PM	SENT