UNITED STATES DISTRICT COURT

FOR THE4 EASTERN DISTRICT OF PENNSYLVANIA

THEODORE TASANGARINOS, Individually and on Behalf of a Class of All Others Similarly Situated, Plaintiff, v. CENCORA, INC. and THE LASH GROUP, LLC, Defendants.	**Case No.** **CLASS ACTION COMPLAINT** **Jury Trial Demanded**

Upon personal knowledge as to his own acts, and based upon his investigation, the investigation of counsel, and information and belief as to all other matters, Plaintiff Theodore Tasangarinos, on behalf of himself and all others similarly situated, alleges as follows:

SUMMARY OF THE ACTION

1. Plaintiff brings this class action against Cencora, Inc. ("Cencora") and The Lash Group, LLC, ("Lash Group," collectively, "Defendants") for their failure to adequately secure and safeguard his and other similarly situation patient's personally identifying information ("PII") and protected health information ("PHI"), including first and last name, date of birth, health diagnosis, and/or medications and prescriptions, from criminal hackers.

2. Defendant Cencora is a pharmaceutical solutions organization that provides medical products and services to patients and healthcare providers, including but not limited to Novartis Pharmaceuticals Corporation and Bristol Myers Squibb. Cencora now operates more than 1,300 locations in 50 countries, and ships more than 6.7 million products daily. Defendant Lash Group is a patient support company owned by Defendant Cencora that provides patient

support services, business analytics and technology services, and other services to pharmaceutical companies.

3. In the ordinary course of providing patient support services to pharmaceutical companies and healthcare, individuals provide Defendants (or Defendants otherwise received) PII and PHI from at least hundreds of thousands of persons. In some instances, there was no outreach on behalf of Defendants seeking a patient's approval to store their PII and PHI in a data repository or notifying the patients of such a practice. In turn, Defendants come into the possession of, and maintain extensive files containing, the PII and PHI of their clients' patients, and owe these individuals an affirmative duty to adequately protect and safeguard this private information against theft and misuse. Despite such duties created by statute, regulation, and common law, at all relevant times, Defendants utilized deficient data security practices, thereby allowing hundreds of thousands of persons' sensitive and private data to fall into the hands of strangers.

4. On February 27, 2024, Cencora filed an official notice of a hacking incident with the U.S. Securities and Exchange Commission in its Form 8-K.[1] Under state and federal law, organizations must report breaches involving PHI within at least sixty (60) days.

5. On or about May 17, 2024, Cencora also sent out data breach letters (the "Notice") to individuals whose information was compromised as a result of the hacking incident.

6. Based on the Notice sent to Plaintiff and the "Class Members" (defined below), unusual activity was detected on some of their computer systems. In response, Defendants launched an investigation. Cencora's investigation revealed that an unauthorized party had access

[1] *See* https://www.sec.gov/Archives/edgar/data/1140859/000110465924028288/tm247267d1_8k.htm, (last visited July 1, 2024).

to certain files that contained sensitive patient information and that such access took place on an undisclosed date (the "Data Breach"). Despite this knowledge, Cencora waited nearly ***three months*** to notify the public that they were at risk.

7. As a result of this delayed response, Plaintiff and Class Members had no idea for approximately three months that their PII and PHI had been compromised, and that they were, and continue to be, at significant risk of identity theft and various other forms of personal, social, and financial harm. The risk will remain for their respective lifetimes.

8. The PII and PHI compromised in the Data Breach contained highly sensitive patient data, representing a treasure trove for hackers and data thieves. The data included, but is not limited to, patients' names, date(s) of birth, addresses, health diagnoses, and/or medications and prescriptions that Defendants collected and maintained.

9. Armed with the PII and PHI accessed in the Data Breach (and a head start), data thieves can perpetrate a variety of crimes including, e.g., opening new financial accounts in Class Members' names, taking out loans in Class Members' names, using Class Members' names to obtain medical services, using Class Members' information to obtain government benefits, filing fraudulent tax returns using Class Members' information, obtaining driver's licenses in Class Members' names but with another person's photograph, and giving false information to police during an arrest.

10. On information and belief, Plaintiff and Class Members were further harmed by Defendants' poor data security, because even the hackers' *attempts* to access patients' PII and PHI disrupted the integrity of other websites, including financial websites, which then blocked Plaintiff and Class Members and required them to create new logins for reasons that were not

obvious to them at the time and that may have further affected Plaintiff and Class Members' credit scores.

11. There has been no assurance offered by Defendants that all personal data or copies of data have been recovered or destroyed, or that Cencora has adequately enhanced their data security practices sufficient to avoid a similar breach of their network in the future.

12. Therefore, Plaintiff and Class Members have suffered and are at an imminent, immediate, and continuing increased risk of suffering, ascertainable losses in the form of harm from identity theft and other fraudulent misuse of their PII and PHI, the loss of the benefit of their bargain, out-of-pocket expenses incurred to remedy or mitigate the effects of the Data Breach, and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach.

13. Plaintiff brings this class action lawsuit to address Defendants' inadequate safeguarding of Class Members' PII and PHI that they collected and maintained, and their failure to provide timely and adequate notice to Plaintiff and Class Members of the types of information accessed, and that such information was subject to unauthorized access by cybercriminals.

14. The potential for improper disclosure and theft of Plaintiff's and Class Members' PII and PHI was a known risk to Defendants, and thus Defendants were on notice that failing to take necessary steps to secure the PII and PHI left them vulnerable to an attack.

15. Plaintiff's and Class Members' identities are now at risk because of Defendants' negligent conduct as the PII and PHI that they collected and maintained is now in the hands of data thieves and other unauthorized third parties.

16. Plaintiff seeks to remedy these harms on behalf of himself and all similarly situated individuals whose PII and PHI was accessed and/or compromised during the Data Breach.

17. Accordingly, Plaintiff, on behalf of himself and the Class, asserts claims for negligence, negligence per se, invasion of privacy, breach of implied contract, unjust enrichment, breach of fiduciary duty, and declaratory / injunctive relief.

PARTIES

A. Plaintiff

18. Plaintiff Theodore Tasangarinos is a resident and citizen of Florida, residing in Tarpon Springs, Florida.

B. Defendant

19. Defendant Cencora, Inc. is an international pharmaceutical solutions organization incorporated in Delaware with their principal place of business located at 1 West First Ave, Conshohocken, Pennsylvania, 19428.

20. Defendant Lash Group is a patient support company owned by Defendant Cencora that provides patient support services, business analytics and technology services, and other services to pharmaceutical companies with their principal place of business located at 1 West First Ave, Conshohocken, Pennsylvania, 19428.

JURISDICTION AND VENUE

21. The Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million, exclusive of interest and costs. Upon information and belief, the number of class members is over 100,

many of whom have different citizenship from Defendants. Thus, minimal diversity exists under 28 U.S.C. § 1332(d)(2)(A).

22. This Court has jurisdiction because Defendants operate in this District.

23. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(a)(1) because a substantial part of the events giving rise to this action occurred in this District and Defendants have harmed Class Members residing in this District.

FACTUAL BACKGROUND

A. Cencora's Business and Collection of Plaintiff's and Class Members' PII and PHI

24. Defendant Cencora is a pharmaceutical solutions organization that provides medical products and services to patients and healthcare providers. Founded in 2001, Defendant Cencora operates more than 1,300 locations in 50 countries,[2] and ships more than 6.7 million products daily.[3]

25. Defendant Lash Group is an affiliate subsidiary of Defendant Cencora.

26. Upon information and belief, Defendant Cencora employs more than 46,000 people and generates approximately $ 262 billion in annual revenue.[4]

27. As a condition of receiving healthcare services, Defendant Cencora requires that their patients entrust it with highly sensitive personal and health information.[5] In the ordinary course of receiving service from Defendant Cencora, Plaintiff and Class Members were required to provide their PII and PHI to Defendants.

---

[2] *See* https://cencoraventures.cencora.com/about-cencora (last visited July 1, 2024).
[3] *See* https://www.cencora.com/-/media/assets/corporate/global/our-impact/dei/ab-fy22-esg-summary-report.pdf at 5 (last visited July 1, 2024).
[4] *See* https://www.cpomagazine.com/cyber-security/pharmaceutical-giant-cencora-confirms-patient-data-breach-impacting-over-a-dozen-pharma-companies/ (last visited July 1, 2024).
[5] *See* https://www.cencora.com/global-privacy-statement-overview (last visited July 1, 2024).

28. In their Privacy Statement, "Cencora, Inc. and their affiliate companies value and protect the personal information entrusted to the company by their suppliers, customers, and visitors."[6] Defendant Cencora also states that it "adopt[s] appropriate security measures to protect the Personal Data we process, including sensitive Personal Data."[7]

29. Thus, due to the highly sensitive and personal nature of the information Defendant Cencora acquires and stores with respect to their patients, Defendant Cencora, upon information and belief, promises to, among other things: keep patients' PII and PHI private; comply with industry standards related to data security and the maintenance of their patients' PII and PHI; inform their patients of their legal duties relating to data security and comply with all federal and state laws protecting patients' PII and PHI; only use and release patients' PII and PHI for reasons that relate to the services it provides; and provide adequate notice to patients if their PII and PHI is disclosed without authorization.

30. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' Private Information, Defendants assumed legal and equitable duties they owed to Plaintiff and the Class and knew or should have known that they were responsible for protecting Plaintiff's and Class Members' PII and PHI from unauthorized disclosure and exfiltration.

31. Plaintiff and Class Members relied on Defendants to keep their PII and PHI confidential and securely maintained and to only make authorized disclosures of this information, which Defendants ultimately failed to do.

[6] *Id*.
[7] *See* https://www.cencora.com/global-privacy-statement (last visited July 1, 2024).

B. The February Data Breach and Defendants' Inadequate Notice to Plaintiff and Class Members

32. According to Defendants' Notice, they learned of unauthorized access to their computer systems on February 21, 2024, with such unauthorized access having taken place on an undisclosed date.

33. Through the Data Breach, the unauthorized cybercriminal(s) accessed a cache of highly sensitive PII and PHI, including patients' names, date(s) of birth, addresses, health diagnoses, medications and/or prescriptions.

34. On or about May 17, 2024, roughly three months after Defendant Cencora learned that the Class's PII and PHI were first accessed by cybercriminals, Defendant Cencora finally began to notify patients that their investigation determined that their PII and PHI were affected.

35. Defendant Cencora had obligations created by contract, industry standards, common law, and representations made to Plaintiff and Class Members to keep Plaintiff's and Class Members' PII and PHI confidential and to protect them from unauthorized access and disclosure.

36. Plaintiff and Class Members provided their PII and PHI to Defendant Cencora with the reasonable expectation and mutual understanding that Defendant Cencora would comply with their obligations to keep such PII and PHI confidential and secure from unauthorized access and to provide timely notice of any security breaches.

37. Defendant Cencora's data security obligations were particularly important given the substantial increase in cyberattacks in recent years.

38. Defendant Cencora knew or should have known that their electronic records would be targeted by cybercriminals.

C. The Healthcare Sector Is Increasingly Susceptible to Data Breaches, Giving Defendants Ample Notice That They Were Likely Cyberattack Targets

39. Defendants were on notice that companies in the healthcare industry are susceptible targets for data breaches.

40. Defendants were also on notice that the FBI has been long concerned about data security in the healthcare industry. 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)."[8]

41. At all relevant times, Defendants knew, or should have known, that the PII and PHI they were entrusted with were prime targets for malicious actors. Defendants knew this given the unique type and the significant volume of data on their networks, servers, and systems, comprising individuals' detailed and confidential personal information and, thus, the significant number of individuals who the exposure of the unencrypted data would harm.

42. As custodian of Plaintiff's and Class Members' PII and PHI, Defendants knew or should have known the importance of protecting their PII and PHI, and of the foreseeable consequences and harms to such persons if any data breach occurred.

43. Defendants' security obligations were especially important due to the substantial increase of cyberattacks and data breaches in recent years, particularly those targeting healthcare

[8] Jim Finkle, *FBI Warns Healthcare Firms that they are Targeted by Hackers*, REUTERS (Aug. 20, 2014), https://www.reuters.com/article/us-cybersecurity- healthcare-fbi/fbi-warns-healthcare-firms-they-are-targeted-by-hackers- idUSKBN0GK24U20140820.

businesses and other organizations like Defendants, which store and maintain large volumes of PII and PHI. These largescale cyberattacks are increasingly common and well-publicized. In 2023, a total of 725 largescale cyberattacks targeted hospitals, health systems, and healthcare records, affecting more than 133 million people—making 2023 the "worst-ever year for breached healthcare records."[9] With the surging number of such attacks targeting companies in the healthcare sector, Defendants knew or should have known that they were at high risk of cyberattack and should have taken additional and stronger precautions and preemptive measures.

D. Defendants Breached Their Duties to Plaintiff and the Class Members and Failed to Comply with Regulatory Requirements and Industry Practices.

44. Because Defendants were entrusted with PII and PHI at all times herein relevant, Defendants owed to Plaintiff and the Class a duty to exercise commercially reasonable methods and care in handling, using, maintaining, storing, and safeguarding the PII and PHI in their care, control, and custody, including by implementing industry-standard security procedures sufficient to reasonably protect the information from the Data Breach, theft, and unauthorized use that occurred, and to promptly detect and thwart attempts at unauthorized access to their networks and systems. Defendants also owed a duty to safeguard PII and PHI because they were on notice that they were handling highly valuable data and knew there was a significant risk it would be targeted by cybercriminals. Furthermore, Defendants knew of the extensive, foreseeable harm that would ensue for the victims of a data breach, and therefore also owed a duty to reasonably safeguard that information.

[9] Steve Alder, *Security Breaches in Healthcare in 2023*, THE HIPAA JOURNAL (Jan. 31, 2024), https://www.hipaajournal.com/security-breaches-in-healthcare/.

45. Security standards commonly accepted among companies like Defendant Cencora, that store PII and PHI include, without limitation:

i. Maintaining a secure firewall configuration;

ii. Monitoring for suspicious or irregular traffic to servers or networks;

iii. Monitoring for suspicious credentials used to access servers or networks;

iv. Monitoring for suspicious or irregular activity by known users;

v. Monitoring for suspicious or unknown users;

vi. Monitoring for suspicious or irregular server requests;

vii. Monitoring for server requests for PII or PHI;

viii. Monitoring for server requests from virtual private networks (VPNs); and

ix. Monitoring for server requests for Tor exit nodes.

46. The U.S. Federal Trade Commission ("FTC") publishes guides for businesses for cybersecurity[10] and protection of PII which includes basic security standards applicable to all types of businesses.[11]

47. The FTC recommends that businesses:

i. Identify all connections to the computers where sensitive information is stored.

ii. Assess the vulnerability of each connection to commonly known or reasonably foreseeable attacks.

[10] Start with Security: A Guide for Business, FTC (June 2015), *available at* https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf.

[11] Protecting Personal Information: A Guide for Business, FTC (Oct. 2016), *available at* https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.

iii. Do not store sensitive consumer data on any computer with an internet connection unless it is essential for conducting their business.

iv. Scan computers on their network to identify and profile the operating system and open network services. If services are not needed, they should be disabled to prevent hacks or other potential security problems. For example, if email service or an internet connection is not necessary on a certain computer, a business should consider closing the ports to those services on that computer to prevent unauthorized access to that machine.

v. Pay particular attention to the security of their web applications—the software used to give information to visitors to their websites and to retrieve information from them. Web applications may be particularly vulnerable to a variety of hacker attacks.

vi. Use a firewall to protect their computers from hacker attacks while it is connected to a network, especially the internet.

vii. Determine whether a border firewall should be installed where the business's network connects to the internet. A border firewall separates the network from the internet and may prevent an attacker from gaining access to a computer on the network where sensitive information is stored. Set access controls—settings that determine which devices and traffic get through the firewall—to allow only trusted devices with a legitimate business need to access the network. Since the protection a firewall provides is only as effective as their access controls, they should be reviewed periodically.

viii. Monitor incoming traffic for signs that someone is trying to hack in. Keep an eye out for activity from new users, multiple log-in attempts from unknown users or computers, and higher-than-average traffic at unusual times of the day.

ix. Monitor outgoing traffic for signs of a data breach. Watch for unexpectedly large amounts of data being transmitted from their system to an unknown user. If large amounts of information are being transmitted from a business's network, the transmission should be investigated to make sure it is authorized.

48. As described further below, Defendants owed a duty to safeguard PII and PHI under several statutes, including the Federal Trade Commission Act, 15 U.S.C. § 45 (the "FTC Act") and as a covered entity under HIPAA, to ensure that all information they received, maintained, and stored was secure. These statutes were enacted to protect Plaintiff and the Class Members from the type of conduct in which Defendants engaged, and the resulting harms Defendants proximately caused Plaintiff and the Class Members.

49. Under the FTC Act, Defendants had a duty to provide fair and adequate computer systems and data security practices to safeguard the PII and PHI of Plaintiff and Class Members. Under HIPAA, 42 U.S.C. § 1320d, and their implementing regulations, 45 C.F.R. §§ 160, *et seq.*, Defendants had a duty to securely store and maintain the PII and PHI of Plaintiff and Class Members which was collected in conjunction with receiving medical services.

50. Defendants breached their duty to exercise reasonable care in protecting Plaintiff's and Class Members' PII and PHI by failing to implement and maintain adequate data security measures to safeguard Plaintiff's and Class Members' sensitive personal information, failing to encrypt or anonymize PII and PHI within their systems and networks, failing to monitor their systems and networks to promptly identify and thwart suspicious activity, failing to delete and purge PII and PHI no longer necessary for their provision of healthcare services to their patients and other persons, allowing unmonitored and unrestricted access to unsecured PII and PHI, and allowing (or failing to prevent) unauthorized access to, and exfiltration of, Plaintiff's and Class

Member's confidential and private information. Additionally, Defendants breached their duty by utilizing outdated and ineffectual data security measures which deviated from standard industry best practices at the time of the Data Breach. Through these actions, Defendants also violated their duties under the FTC Act and HIPAA.

51. Defendants failed to prevent the Data Breach. Had Defendants properly maintained and adequately protected their systems, servers, and networks, the Data Breach would not have occurred.

52. Additionally, the law imposes an affirmative duty on Defendants to timely disclose the unauthorized access and theft of PII and PHI to Plaintiff and Class Members so that they can take appropriate measures to mitigate damages, protect against adverse consequences, and thwart future misuses of their private information. Defendants further breached their duties by failing to provide reasonably timely notice of the Data Breach to Plaintiff and Class Members. In so doing, Defendants actually and proximately caused and exacerbated the harm from the Data Breach and the injuries-in-fact of Plaintiff and Class Members.

E. The Experiences of Plaintiff Theodore Tasangarinos

53. Plaintiff received notice of the Data Breach by letter from Cencora, Inc. dated May 17, 2024. At various relevant times, Plaintiff received healthcare services from Bristol Myers Squibb and/or the Bristol Myers Squibb Patient Assistance Foundation, a client of the Lash Group LLC, which was referenced in the May 17, 2024 notice.

54. Plaintiff also received notice of the Data Breach by letter from Cencora, Inc. dated May 22, 2024. At various relevant times, Plaintiff received healthcare services from Novartis Pharmaceuticals Corporation, a client of Cencora, Inc., which was referenced in the May 2, 2024 notice.

55. As a proximate result of the Data Breach, Plaintiff has spent time and will continue to spend time for the foreseeable future and beyond dealing with the Data Breach's consequences, including by and self-monitoring his accounts and credit reports to monitor potentially suspicious and fraudulent activity. This time has been and will continue to be lost forever and cannot be recaptured.

56. Plaintiff has experienced distress, anxiety and stress because his personal information was compromised in the Data Breach, the uncertainty surrounding how Defendants came to possess his information in the first instance, and not knowing who stole his information or for what purpose. Plaintiff's anxiety stems from the fact that there was never any outreach on behalf of Defendants seeking Plaintiff's approval to store his PII and PHI in a data repository, nor did Plaintiff receive notice of such a practice. This goes beyond allegations of mere worry or inconvenience; it is exactly the sort of injury and harm to a data breach victim that the law contemplates and addresses.

57. Plaintiff has also observed unexplained anomalies in his credit report since the Data Breach, which on information and belief resulted from the Data Breach, and which are negatively affecting his credit, business and livelihood.

58. Plaintiff suffered actual injuries in the form of damages to and diminution in the value of his PII and PHI—a form of intangible property that was entrusted to Defendants, which was compromised in and as a proximate result of the Data Breach.

59. Plaintiff has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse proximately resulting from his PII and PHI being obtained by unauthorized third parties and possibly cybercriminals.

60. Plaintiff has a continuing interest in ensuring that his PII and PHI, which remains within Defendants' possession and control, are protected and safeguarded against future data breaches or cybersecurity risks.

61. Defendants deprived Plaintiff of the earliest opportunity to guard himself against the Data Breach's harmful effects by failing to promptly notify him about it. Instead, ***Defendants waited three months***, without any explanation whatsoever.

F. Plaintiff the Class Suffered Actual and Impending Injuries Resulting from the Data Breach

62. As a proximate result of Defendants' completely unreasonable security practices, identity thieves now possess the sensitive PII and PHI of Plaintiff and the Class. That information is extraordinarily valuable on the black market and incurs direct costs to Plaintiff and the Class. On the dark web—an underground internet black market—criminals openly buy and sell stolen PII and PHI to create "identity kits" worth up to $2,000 each that can be used to create fake IDs, gain access to bank accounts, social media accounts, and credit cards, file false insurance claims or tax returns, or rack up other kinds of expenses.[12] And, "[t]he damage to affected [persons] may never be undone."[13]

63. Unlike the simple credit card breaches at retail merchants, these damages cannot be avoided by canceling and reissuing plastic cards or closing an account. Identity theft is far more pernicious than credit card fraud. Criminals' ability to open entirely new accounts—not simply

[12] Nick Culbertson, *Increased Cyberattacks on Healthcare Institutions Shows the Need for Greater Cybersecurity* (Jun. 7, 2021), FORBES, https://www.forbes.com/sites/forbestechcouncil/2021/06/07/increased-cyberattacks-on-healthcare-institutions-shows-the-need-for-greater-cybersecurity/?sh=ca928c05650d.

[13] *Id.*

prey on existing ones—poses far more dangerous problems. Identity thieves can retain the stolen information for years until the controversy has receded because victims may become less vigilant in monitoring their accounts as time passes. Then, at any moment, the thief can take control of a victim's identity, resulting in thousands of dollars in losses and lost productivity. The U.S. Department of Justice has reported that in 2021, identity theft victims spent on average about four hours to resolve problems stemming therefrom and that the average financial loss experienced by an identity theft victim was $1,160 per person.[14] Additionally, about 80% of identity theft victims reported some form of emotional distress resulting from the incident.[15]

64. As a consequence of the Data Breach, Plaintiff's and Class Members' credit profiles can be destroyed before they even realize what happened, and they may be unable to legitimately borrow money, obtain credit, or open bank accounts. Plaintiff and Class Members can be deprived of legitimate tax refunds or, worse yet, may face state or federal tax investigations due to fraud committed by an identity thief. And even the simple preventive step of adding oneself to a credit-fraud watch list to guard against these consequences substantially impairs Plaintiff's and Class Members' ability to obtain additional credit. In fact, many experts advise victims to place a freeze on all credit accounts, making it impossible to rent a car, get student loans, buy or rent big-ticket items, or complete a major new car or home purchase.

65. Cybercriminals sell health information at a far higher premium than stand-alone PII. This is because health information enables thieves to go beyond traditional identity theft and

[14] Erika Harrell and Alexandra Thompson, Victims of Identity Theft, 2021, U.S. DEPARTMENT OF JUSTICE, OFFICE OF JUSTICE PROGRAMS, BUREAU OF JUSTICE STATISTICS (Oct. 2023), *available at* https://bjs.ojp.gov/document/vit21.pdf.

[15] *Id.*

obtain medical treatments, purchase prescription drugs, submit false bills to insurance companies, or even undergo surgery under a false identity.[16] The shelf life for this information is also much longer—while individuals can update their credit card numbers, they are less likely to change their health insurance information. When medical identity theft occurs, the associated costs to victims can be exorbitant. According to a 2015 study, at least 65% of medical identity theft victims had to "pay an average of $13,500 to resolve the crime."[17]

66. Defendants' Data Breach notices to affected persons do not provide adequate remediation and compensation for their wrongful conduct and actions described herein. Therein, Defendants state that they "apologize[] for the concern and inconvenience" the incident may cause, yet only offered affected individuals complimentary identity protection service through their hand-picked vendor, Experian IdentityWorks, for 24 months.[18]

CLASS ACTION ALLEGATIONS

67. Pursuant to Federal Rule of Civil Procedure 23(b)(2) and (b)(3), as applicable, and (c)(4), Plaintiff seek certification of the following nationwide class (the "Class"):

> All persons whose PII or PHI was compromised in the Data Breach discovered by Cencora, Inc. and/or the Lash Group LLC on or about February 21, 2024, including all persons who were sent a notice of the Data Breach (and each person a "Class Member").

68. Excluded from the Class are any entity in which Defendants have a controlling interest, and Defendants' officers, directors, affiliates, legal representatives, co-conspirators,

[16] Medical Identity Theft: FAQs for Health Care Providers and Health Plans, FTC, *available at* https://www.ftc.gov/system/files/documents/plain-language/bus75-medical-identity-theft-faq-health-care-health-plan.pdf.

[17] Justin Klawans, *What is medical identity theft and how can you avoid it?*, THE WEEK (Aug. 2, 2023), https://theweek.com/feature/briefing/1025328/medical-identity-theft-how-to-avoid.

[18] *See* https://www.cpomagazine.com/cyber-security/pharmaceutical-giant-cencora-confirms-patient-data-breach-impacting-over-a-dozen-pharma-companies/ (last visited July 1, 2024).

successors, subsidiaries, and assigns. Also excluded from the Class are any judges, justices, or judicial officers presiding over this matter and the members of their immediate families and judicial staff.

69. This action is brought and may be properly maintained as a class action pursuant to Federal Rule of Civil Procedure 23(b)(2) and 23(b)(3), and satisfies the numerosity, commonality, typicality, adequacy, predominance, and superiority requirements of these rules.

70. ***Numerosity Under Rule 23(a)(1).*** The Class is so numerous that the individual joinder of all members is impracticable, and the disposition of the claims of all members of the Class in a single action will provide substantial benefits to the parties and the Court. Although the precise number of members of the Class is unknown to Plaintiff at this time, on information and belief, the proposed Class contains at least 540,000 individuals.[19] Discovery will reveal, through Defendants' records, the actual number of members of the Class.

71. ***Commonality Under Rule 23(a)(2).*** Common legal and factual questions exist that predominate over any questions affecting only individual members of the Class. These common questions, which do not vary among members of the Class, and which may be determined without reference to any Class member's individual circumstances, include, but are not limited to:

(a) Whether Defendants knew or should have known that their computer systems and networks were vulnerable to unauthorized third-party access or a cyberattack;

(b) Whether Defendants failed to utilize and maintain adequate and reasonable security and preventive measures to ensure that their computer systems and networks were protected;

[19] *See* https://www.cpomagazine.com/cyber-security/pharmaceutical-giant-cencora-confirms-patient-data-breach-impacting-over-a-dozen-pharma-companies/ (last visited July 1, 2024).

(c) Whether Defendants failed to take available steps to prevent and stop the Data Breach from occurring;

(d) Whether Defendants owed a legal duty to Plaintiff and Class Members to protect their PII and PHI;

(e) Whether Defendants breached any duty to protect the PII or PHI of Plaintiff and Class Members by failing to exercise due care in protecting their sensitive and private information;

(f) Whether Defendants provided timely, accurate, and sufficient notice of the Data Breach to Plaintiff and the Class Members;

(g) Whether Plaintiff and Class Members have been damaged by the wrongs alleged and are entitled to actual, statutory, or other forms of damages and other monetary relief; and

(h) Whether Plaintiff and Class Members are entitled to injunctive or equitable relief, including restitution.

72. ***Typicality Under Rule 23(a)(3).*** Plaintiff's claims are typical of the claims of the Class. Plaintiff, like all proposed members of the Class, had his PII or PHI compromised in the Data Breach. Defendants' uniformly unlawful course of conduct injured Plaintiff and Class Members in the same wrongful acts and practices. Likewise, Plaintiff and other Class Members must prove the same facts in order to establish the same claims.

73. ***Adequacy of Representation Under Rule 23(a)(4).*** Plaintiff is an adequate representative of the Class because his interests do not conflict with the interests of the Class. Plaintiff has retained counsel competent and experienced in complex litigation, data breach cases, and consumer protection class action matters such as this action, and Plaintiff and his counsel intend to vigorously prosecute this action for the Class's benefit and have the resources to do so. Plaintiff and his counsel have no interests adverse to those of the other members of the Class.

74. ***Predominance and Superiority.*** A class action is superior to all other available methods for the fair and efficient adjudication of this controversy because individual litigation of each Class Member's claim is impracticable. The damages, harm, and losses suffered by the individual members of the Class will likely be small relative to the burden and expense of individual prosecution of the complex litigation necessitated by Defendants' wrongful conduct. Even if each Class Member could afford individual litigation, the Court system could not. It would be unduly burdensome if tens of thousands of individual cases or more proceeded. Individual litigation also presents the potential for inconsistent or contradictory judgments, the prospect of a race to the courthouse, and the risk of an inequitable allocation of recovery among those individuals with equally meritorious claims. Individual litigation would increase the expense and delay to all parties and the Courts because it requires individual resolution of common legal and factual questions. By contrast, the class action device presents far fewer management difficulties and provides the benefit of a single adjudication, economies of scale, and comprehensive supervision by a single court.

75. Finally, all members of the proposed Class are readily ascertainable. Defendant Cencora has access to the names and addresses and/or email addresses of Class Members affected by the Data Breach through its books and records. Class Members have already been preliminarily identified and sent notice of the Data Breach by Defendant Cencora.

76. As a result of the foregoing, class treatment under Federal Rule of Civil Procedure 23 is appropriate.

FIRST CLAIM FOR RELIEF
Negligence
(On Behalf of Plaintiff and the Nationwide Class)

77. Plaintiff incorporates by reference and realleges paragraphs 1-75 as if fully set forth herein.

78. In the ordinary course of providing healthcare services to their patients and other individuals and employing their staff, Defendants solicited, gathered, and stored the PII and PHI of Plaintiff and Class Members. Because Defendants were entrusted with such PII and PHI at all times herein relevant, they owed to Plaintiff and the Class a duty to exercise commercially reasonable methods and care in handling, using, maintaining, storing, and safeguarding the PII and PHI in their care, control, and custody, including by implementing industry-standard security procedures sufficient to reasonably protect the information from the Data Breach, theft, and unauthorized use that occurred, and to promptly detect and thwart attempts at unauthorized access to their networks and systems. This duty arose independently from any contract.

79. Defendants knew, or should have known, of the risks inherent in collecting and storing massive amounts of PII and PHI, including the importance of adequate data security and the high frequency of ransomware attacks and well-publicized data breaches both generally and the increasing rate of cybercriminals specifically targeting the healthcare industry, like Defendants. Defendants owed a duty of care to Plaintiff and Class Members because it was foreseeable that their failure to adequately safeguard their PII and PHI in accordance with state-of-the-art industry standards concerning data security would result in the compromise of that sensitive information. Defendants acted with wanton and reckless disregard for the security and confidentiality of Plaintiff's and the Class's PII and PHI by failing to limit access to this information to unauthorized

third parties and by not properly supervising both the way the PII and PHI were stored, used, and exchanged, and those in their employ responsible for such tasks.

80. Defendants owed to Plaintiff and members of the Class a duty to notify them within a reasonable timeframe of any breach to the security of their PII and PHI. Defendants also owed a duty to timely and accurately disclose to Plaintiff and Class Members the scope, nature, and circumstances of the Data Breach. This duty is required and necessary for Plaintiff and the Class to take appropriate measures to protect their PII and PHI, to be vigilant in the face of an increased risk of harm, and to take other necessary steps to mitigate the harm caused by the Data Breach.

81. Defendants also had a common law duty to prevent foreseeable harm to others. Defendants had full knowledge of the sensitivity and high value of the PII and PHI that they stored and the types of foreseeable harm and injury-in-fact that Plaintiff and Class Members could and would suffer if that PII and PHI were wrongfully disclosed, leaked, accessed, or exfiltrated. Defendants' conduct created a foreseeable and unreasonable risk of harm to Plaintiff and Class Members, who were the foreseeable victims of Defendants' inadequate data security practices.

82. Defendants violated their duty to implement and maintain reasonable security procedures and practices, including through their failure to adequately restrict access to their file systems and networks that held hundreds of thousands of individuals' PII and PHI or encrypt or anonymize such data. Defendants' duty included, among other things, designing, maintaining, and testing Defendant Cencora and Defendant Lash Group's information security controls to ensure that PII and PHI in their possession were adequately secured by, for example, encrypting or anonymizing sensitive personal information, installing intrusion detection and deterrent systems and monitoring mechanisms, and using access controls to limit access to sensitive data.

83. Defendants' duty of care also arose by operation of statute, as follows:

a. Pursuant to the FTC Act, 15 U.S.C. § 45, Defendants had a duty to provide fair and adequate computer systems and data security practices to safeguard the PII and PHI of Plaintiff and Class Members; and

b. Pursuant to HIPAA, 42 U.S.C. § 1320d, and their implementing regulations, 45 C.F.R. §§ 160, *et seq.*, Defendants had a duty to securely store and maintain the PII and PHI of Plaintiff and Class Members which was collected in conjunction with receiving healthcare services. Additionally, the HIPAA Breach Notification Rule, 45 C.F.R. § 164.400-414, required Defendants to provide notice of the Data Breach to each affected individual "without unreasonable delay and in no case later than 60 days following discovery of the breach."

84. These statutes—the FTC Act and HIPAA—were enacted to protect Plaintiff and the Class Members from the type of wrongful conduct in which Defendants engaged.

85. Defendants breached their duty to exercise reasonable care in protecting Plaintiff's' and Class Members' PII and PHI by failing to implement and maintain adequate data security measures to safeguard Plaintiff's and Class Members' sensitive personal information, failing to encrypt or anonymize PII and PHI within their systems and networks, failing to monitor their systems and networks to promptly identify and thwart suspicious activity, failing to delete and purge PII and PHI no longer necessary for their provision of healthcare services to their patients, other persons, and persons within their employ, allowing unmonitored and unrestricted access to unsecured PII and PHI, and allowing (or failing to prevent) unauthorized access to, and copying and exfiltration of, Plaintiff's and Class Members' confidential and private information. Additionally, Defendants breached their duty by utilizing outdated and ineffectual data security measures that deviated from standard industry best practices at the time of the Data Breach. Through these actions, Defendants also violated their duties under the FTC Act and HIPAA.

86. The law imposes an affirmative duty on Defendants to timely disclose the unauthorized access and theft of PII and PHI to Plaintiff and Class Members so that they can take appropriate measures to mitigate damages, protect against adverse consequences, and thwart future misuses of their private information. Defendants further breached their duties by failing to provide such reasonably timely notice of the Data Breach to Plaintiff and Class Members, including by violating the HIPAA Breach Notification Rule. In so doing, Defendants actually and proximately caused and exacerbated the harm from the Data Breach and the injuries-in-fact of Plaintiff and Class Members. Timely disclosure was necessary so that Plaintiff and Class Members could, among other things: (i) purchase identity theft protection, monitoring, and recovery services; (ii) flag asset, credit, and tax accounts for fraud; (iii) purchase or otherwise obtain credit reports; (iv) place or renew fraud alerts on a quarterly basis; (v) closely monitor loan data and public records; and (vi) take other meaningful steps to protect themselves and attempt to avoid or recover from identity theft and other harms.

87. As stated in Defendant Cencora's November 2, 2023, Form 8-K, its revenue was at $262.2 billion for the fiscal year. As such, it had the financial and personnel resources necessary to prevent the Data Breach. Defendants nevertheless failed to adopt reasonable data security measures, in breach of the duties it owed to Plaintiff and Class Members.

88. Plaintiff and Class Members had no ability to protect their PII and PHI once it was in Defendants' possession and control. Defendants were in an exclusive position to protect against the harm suffered by Plaintiff and Class Members as a result of the Data Breach.

89. But for Defendants' breach of their duty to adequately protect Class Members' PII and PHI, Class Members' PII and PHI would not have been stolen. As a result of Defendants' negligence, Plaintiff and Class Members suffered and will continue to suffer the various types of

damages alleged herein. There is a temporal and close causal connection between Defendants' failure to implement adequate data security measures, the Data Breach, and the harms suffered by Plaintiff and Class Members.

90. As a direct and traceable result of Defendants' negligence, Plaintiff and the Class have suffered or will suffer an increased and impending risk of fraud, identity theft, damages, embarrassment, humiliation, frustration, emotional distress, and lost time and out-of-pocket costs to mitigate and remediate the effects of the Data Breach. These harms to Plaintiff and the Class include, without limitation: (i) loss of the opportunity to control how their personal information is used; (ii) diminution in the value and use of their personal information entrusted to Defendants; (iii) the compromise and theft of their personal information; (iv) out-of-pocket costs associated with the prevention, detection, and recovery from identity theft and unauthorized use of financial accounts; (v) costs associated with the ability to use credit and assets frozen or flagged due to credit misuse, including increased costs to use credit, credit scores, credit reports, and assets; (vi) unauthorized use of compromised personal information to open new financial and other accounts; (vii) continued risk to their personal information, which remains in Defendants' possession and is subject to further breaches so long as Defendants fail to undertake appropriate and adequate measures to protect the personal information in their possession; and (viii) future costs in the form of time, effort, and money they will expend to prevent, detect, contest, and repair the adverse effects of their personal information being stolen in the Data Breach.

91. Defendants' negligence was gross, willful, wanton, and warrants the imposition of punitive damages given the clear foreseeability of a hacking incident, the extreme sensitivity of the private information under Defendants' care, and their failure to take adequate remedial steps, including prompt notification of the victims, following the Data Breach.

92. Plaintiff and Class Members are entitled to all forms of monetary compensation set forth herein, including monetary payments to provide adequate long-term identity protection services. Plaintiff and Class Members are also entitled to the injunctive relief sought herein.

SECOND CLAIM FOR RELIEF
Negligence *Per Se*
(On Behalf of Plaintiff and the Nationwide Class)

93. Plaintiff incorporates by reference and realleges paragraphs 1-75 as if fully set forth herein.

94. Pursuant to the FTC Act, 15 U.S.C. § 45, Defendants had a duty to maintain fair and adequate computer systems and data security practices to safeguard Plaintiff's and the Class's PII and PHI.

95. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect customers' PII. The FTC publications and orders promulgated pursuant to the FTC Act also form part of the basis of Defendants' duty to protect Plaintiff's and the Class Members' PII and PHI.

96. Pursuant to HIPAA, 42 U.S.C. §§ 1302, *et seq.*, Defendants also owed Plaintiff and Class Members a duty to provide adequate data security practices and to safeguard their PII and PHI.

97. Defendants' duty to use reasonable care in protecting confidential and sensitive data arose not only as a result of the statutes and regulations described above, but also because Defendants are bound by industry standards to protect confidential PII and PHI.

98. Defendants violated their duties under Section 5 of the FTC Act and HIPAA by failing to use reasonable or adequate data security practices and measures to protect Plaintiff's and

the Class's PII and PHI and not complying with applicable industry standards as described in detail herein. Defendants' conduct was particularly unreasonable given the nature and amount of PII and PHI that Defendants collected and stored and the foreseeable consequences of a cybersecurity data breach, including, specifically, the immense damages that would result to individuals in the event of a breach, which ultimately came to pass.

99. The harm that has occurred is the type of harm the FTC Act and HIPAA are intended to guard against. Indeed, the FTC has pursued numerous enforcement actions against businesses that, because of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and the Class.

100. But for Defendants' wrongful and negligent breach of the duties owed to Plaintiff and Class Members, Plaintiff and the Class Members would not have been injured.

101. The injuries and harms suffered by Plaintiff and the Class Members were the reasonably foreseeable result of Defendants' breach of their duties. Defendants knew or should have known that they were failing to meet their duties and that their breach would cause Plaintiff and the Class Members to suffer the foreseeable harms associated with the exposure of their PII and PHI.

102. Defendants' various violations and their failure to comply with the applicable laws and regulations referenced above constitute negligence *per se*.

103. As a direct and proximate result of Defendants' negligence *per se*, Plaintiff and the Class have suffered harm, including loss of time and money resolving fraudulent charges; loss of time and money obtaining protections against future identity theft; lost control over the value of PII and PHI; harm resulting from damaged credit scores and information; and other harm resulting

from the unauthorized use or threat of unauthorized use of stolen PII and PHI, entitling them to damages in an amount to be proven at trial.

104. Additionally, as a direct and proximate result of Defendants' negligence *per se*, Plaintiff and Class Members have suffered and will suffer the continued risks of exposure of their PII and PHI, which remain in Defendants' possession and are subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the PII and PHI in their continued possession.

THIRD CLAIM FOR RELIEF
Invasion of Privacy
(On Behalf of Plaintiff and the Nationwide Class)

105. Plaintiff incorporates by reference and realleges paragraphs 1-75 as if fully set forth herein.

106. Plaintiff and Class Members have a legally protected privacy interest in their PII and PHI, which is and was collected, stored, and maintained by Defendants, and they are entitled to the reasonable and adequate protection of their PII and PHI against foreseeable unauthorized access, as occurred with the Data Breach.

107. Plaintiff and Class Members reasonably expected that Defendants would protect and secure their PII and PHI from unauthorized parties and that their private information would not be accessed, exfiltrated, and disclosed to any unauthorized parties or for any improper purpose.

108. Defendants unlawfully invaded the privacy rights of Plaintiff and Class Members by engaging in the wrongful conduct described above, including by failing to protect their PII and PHI by permitting unauthorized third parties to access, exfiltrate, copy, and view this private information. Likewise, Defendants further invaded the privacy rights of Plaintiff and Class Members and permitted cybercriminals to invade the privacy rights of Plaintiff and Class

Members, by unreasonably and intentionally delaying disclosure of the Data Breach, and failing to properly identify what PII and PHI had been accessed, exfiltrated, copied, and viewed by unauthorized third parties.

109. This invasion of privacy resulted from Defendants' failure to properly secure and maintain Plaintiff's and the Class Members' PII and PHI, leading to the foreseeable unauthorized access, exfiltration, and disclosure of this unguarded data.

110. Plaintiff's and the Class Members' PII and PHI is the type of sensitive, personal information that one normally expects will be protected from exposure by the very entity charged with safeguarding it. Further, the public has no legitimate concern in Plaintiff's and the Class Members' PII and PHI, and such private information is otherwise protected from exposure to the public by various statutes, regulations, and other laws.

111. The disclosure of Plaintiff's and the Class Members' PII and PHI to unauthorized parties is substantial and unreasonable enough to be legally cognizable and is highly offensive to a reasonable person.

112. Defendants' willful and reckless conduct which permitted unauthorized access, exfiltration and disclosure of Plaintiff's and the Class Members' sensitive, PII and PHI is such that it would cause serious mental injury, shame, embarrassment, or humiliation to people of ordinary sensibilities.

113. The unauthorized access, exfiltration, and disclosure of Plaintiff's and the Class Members' PII and PHI was without their consent, and in violation of various statutes, regulations, and other laws.

114. As a result of the invasion of privacy caused by Defendants, Plaintiff and the Class Members suffered and will continue to suffer damages and injuries as set forth herein.

115. Plaintiff and the Class Members seek all monetary and non-monetary relief allowed by law, including damages, punitive damages, restitution, injunctive relief, reasonable attorneys' fees and costs, and any other relief that the Court deems just and proper.

FOURTH CAUSE OF ACTION
Breach of Implied Contract
(On Behalf of Plaintiff and the Nationwide Class)

116. Plaintiff incorporates by reference and realleges paragraphs 1-75 as if fully set forth herein.

117. This claim is pleaded in the alternative to Plaintiff's unjust enrichment and quasi-contract claim, *infra*.

118. Through their course of conduct, Plaintiff and the Class Members entered into implied contracts with Defendants under which Defendants agreed to safeguard and protect their confidential and private PII and PHI and to timely and accurately notify Plaintiff and Class Members if their information had been breached and compromised.

119. Defendants acquired, stored, and maintained the PII and PHI of Plaintiff and the Class that they received either directly from them or that Defendants otherwise received from other third parties.

120. Plaintiff and Class Members were required to provide, or authorize the transfer of, their private information and health information for Defendants to provide their pharmaceutical or healthcare services, or for purposes of employment. Plaintiff and Class Members paid money, or money was paid on their behalf, or provided services to Defendants in exchange for such services.

121. Defendants solicited, offered, and invited Class Members to provide their private information and health information as part of Defendants' regular business practices. Plaintiff and

Class Members accepted Defendants' offers and provided their private information and health information to Defendants.

122. Defendants accepted possession of Plaintiff's and Class Members' PII and PHI for the purpose of providing pharmaceutical or healthcare services to Plaintiff and Class Members.

123. When Plaintiff and Class Members paid money and provided their PII and PHI to Defendants and their healthcare providers, either directly or indirectly, in exchange for pharmaceutical or healthcare services, they entered into implied contracts with their healthcare providers and their business associates, including Defendants, and intended and understood that PII and PHI would be adequately safeguarded as part of that service. Alternatively, Plaintiff and Class Members are the intended third-party beneficiaries of data protection agreements entered into between Defendants and their healthcare provider clients.

124. Defendants' implied promise of confidentiality to Plaintiff and Class Members includes consideration beyond those pre-existing general duties owed under the FTC Act, HIPAA, or other state or federal regulations. The additional consideration included implied promises to take adequate steps to comply with specific industry data security standards and FTC guidelines on data security.

125. Defendants' implied promises include but are not limited to: (a) taking steps to ensure that any agents who are granted access to PII and PHI also protect the confidentiality of that data; (b) taking steps to ensure that the information that is placed in the control of their agents is restricted and limited to achieve an authorized medical purpose; (c) restricting access to qualified and trained agents; (d) designing and implementing appropriate retention policies to protect the information against criminal data breaches; (e) applying or requiring proper encryption; (f)

multifactor authentication for access; and (g) other steps to protect against foreseeable data breaches.

126. Defendants' implied promises to Plaintiff and Class Members include, but are not limited to, (1) taking steps to ensure that anyone who is granted access to their PII and PHI will also protect the confidentiality of that data; (2) taking steps to ensure that the PII and PHI that is placed in the control of their employees is restricted and limited to achieve an authorized business purpose; (3) restricting access to qualified and trained employees and/or agents; (4) designing and implementing appropriate retention policies to protect the PII and PHI against criminal data breaches; (5) applying or requiring proper encryption; (6) implementing multifactor authentication for access; (7) complying with HIPAA standards to make sure that Plaintiff's and Class Members' PHI would remain protected; and (8) taking other steps to protect against foreseeable data breaches.

127. Plaintiff and the Class Members would not have entrusted their PII and PHI to Defendants in the absence of such an implied contract. Had Defendants disclosed to Plaintiff and the Class (or their physicians and other healthcare providers) that they did not have adequate computer systems and security practices to secure sensitive data, Plaintiff and the other Class Members (or their physicians and healthcare providers) would not have provided their PII and PHI to Defendants.

128. Defendants recognized that Plaintiff's and Class Members' PII and PHI is highly sensitive and must be protected, and that this protection was of material importance as part of the bargain to Plaintiff and the other Class Members.

129. Plaintiff and the Class Members fully and adequately performed their obligations under the implied contracts with Defendants.

130. Defendants breached the implied contracts they made with Plaintiff and the Class Members by failing to take reasonable measures to safeguard their PII and PHI as described herein, as well as by failing to provide accurate, adequate, and timely notice to them that their PII and PHI was compromised as a result of the Data Breach.

131. As a direct and proximate result of Defendants' wrongful conduct, Plaintiff and the other Class Members suffered and will continue to suffer damages in an amount to be proven at trial, or alternatively, nominal damages. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendants to strengthen their data security systems, submit to future audits of those systems, and provide adequate long-term credit monitoring and identity theft protection services to all persons affected by the Data Breach.

FIFTH CLAIM FOR RELIEF
Unjust Enrichment / Quasi-Contract
(On Behalf of Plaintiff and the Nationwide Class)

132. Plaintiff incorporates by reference and realleges paragraphs 1-75 as if fully set forth herein.

133. This claim is pleaded in the alternative to Plaintiff's breach of implied contract claim, *supra*.

134. A monetary benefit was directly and indirectly conferred upon Defendants through their receipt of Plaintiff's and Class Members' PII and PHI, which Defendants used to facilitate the provision of healthcare services or for purposes of employment. Defendants appreciated or had knowledge of these benefits conferred upon them by Plaintiff and the Class.

135. Under principles of equity and good conscience, Defendants should not be permitted to retain the full monetary value of the benefits because Defendants failed to adequately protect Plaintiff's and Class Members' PII and PHI.

136. Plaintiff and the Class Members have no adequate remedy at law. Defendants continue to retain their PII and PHI while exposing this sensitive and private information to a risk of future data breaches while in Defendants' possession. Defendants also continue to derive a financial benefit from using Plaintiff's and Class Members' PII and PHI.

137. As a direct and proximate result of Defendants' wrongful conduct, Plaintiff and the Class Members have suffered various types of damages alleged herein.

138. Defendants should be compelled to disgorge into a common fund for the benefit of Plaintiff and Class Members all unlawful or inequitable proceeds received by them because of their misconduct described herein and the Data Breach.

SIXTH CLAIM FOR RELIEF
Breach of Fiduciary Duty
(On Behalf of Plaintiff and the Nationwide Class)

139. Plaintiff incorporates by reference and realleges paragraphs 1-75 as if fully set forth herein.

140. In light of the special relationship between Defendants and their clients' patients, whereby Defendants became a guardian of Plaintiff's and Class Members' PII and PHI, Defendants were a fiduciary, created by their undertaking and guardianship of the PII and PHI, to act primarily for the benefit of their patients, including Plaintiff and Class Members. This benefit included (1) the safeguarding of Plaintiff's and Class Members' PII and PHI; (2) timely notifying Plaintiff and Class Members of the Data Breach; and (3) maintaining complete and accurate records of what and where Defendants' clients' patients PII and PHI was and is stored.

141. Defendants had a fiduciary duty to act for the benefit of Plaintiff and the Class upon matters within the scope of their clients' patients' relationship, in particular to keep the PII and PHI secure.

142. Defendants breached their fiduciary duties to Plaintiff and Class Members by failing to diligently investigate the Data Breach to determine the number of Class Members affected and notify them within a reasonable and practicable period of time.

143. Defendants breached their fiduciary duties to Plaintiff and the Class by failing to protect their PII and PHI.

144. Defendants breached their fiduciary duties to Plaintiff and Class Members by failing to ensure the confidentiality and integrity of electronic PHI Defendants created, received, maintained, and transmitted, in violation of 45 CFR 164.306(a)(1).

145. Defendants breached their fiduciary duties to Plaintiff and Class Members by failing to implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights, in violation of 45 CFR 164.312(a)(1).

146. Defendants breached their fiduciary duties to Plaintiff and Class Members by failing to implement policies and procedures to prevent, detect, contain, and correct security violations, in violation of 45 CFR 164.308(a)(1).

147. Defendants breached their fiduciary duties to Plaintiff and Class Members by failing to identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity, in violation of 45 CFR 164.308(a)(6)(ii).

148. Defendants breached their fiduciary duties to Plaintiff and Class Members by failing to protect against any reasonably-anticipated threats or hazards to the security or integrity of electronic PHI, in violation of 45 CFR 164.306(a)(2).

149. Defendants breached their fiduciary duties to Plaintiff and Class Members by failing to protect against any reasonably-anticipated uses or disclosures of electronic PHI that are not permitted under the privacy rules regarding individually identifiable health information, in violation of 45 CFR 164.306(a)(3).

150. Defendants breached their fiduciary duties to Plaintiff and Class Members by failing to ensure compliance with the HIPAA security standard rules by their workforce, in violation of 45 CFR 164.306(a)(94).

151. Defendants breached their fiduciary duties to Plaintiff and Class Members by impermissibly and improperly using and disclosing PHI that is and remains accessible to unauthorized persons, in violation of 45 CFR 164.502, *et seq*.

152. As a direct and proximate result of Defendants' breaches of their fiduciary duties, Plaintiff and Class Members have suffered and will continue to suffer the harms and injuries alleged herein, as well as anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

SEVENTH CLAIM FOR RELIEF
Injunctive/Declaratory Relief
(On Behalf of Plaintiff and the Nationwide Class)

153. Plaintiff incorporates by reference and realleges paragraphs 1-75 as if fully set forth herein.

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

155. Defendants owe a duty of care to Plaintiff and Class Members, which required Defendants to adequately monitor and safeguard Plaintiff's and Class Members' PII and PHI.

156. Defendants and their officers, directors, affiliates, legal representatives, employees, co-conspirators, successors, subsidiaries, and assigns still possess the PII and PHI belonging to Plaintiff and Class Members.

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

158. Under their authority pursuant to the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. Defendants owe a legal duty to secure the PII and PHI of Plaintiff and the Class within their care, custody, and control under common law, HIPAA, and Section 5 of FTC Act;

b. Defendants breached their duty to Plaintiff and the Class by allowing the Data Breach to occur;

c. Defendants' existing data monitoring measures do not comply with their obligations and duties of care to provide reasonable security procedures and practices that are appropriate to protect the PII and PHI of Plaintiff and the Class within Defendants' custody, care, and control; and

d. Defendants' ongoing breaches of said duties continue to cause harm to Plaintiff and the Class.

159. This Court should also issue corresponding prospective injunctive relief requiring Defendants to employ adequate security protocols consistent with legal and industry standards to protect the PII and PHI of Plaintiff and the Class within their custody, care, and control, including the following:

a. Order Defendants to provide lifetime credit monitoring and identity theft insurance to Plaintiff and Class Members.

b. Order that, to comply with Defendants' obligations and duties of care, Defendants must implement and maintain reasonable security and monitoring measures, including, but not limited to:

i. Engaging third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendants' systems, networks, and servers on a periodic basis, and ordering Defendants to promptly correct any problems or issues detected by such third-party security auditors;

ii. Encrypting and anonymizing the existing PII and PHI within their servers, networks, and systems to the extent practicable, and purging all such information which is no longer reasonably necessary for Defendants to provide adequate healthcare services to their patients and other persons;

iii. Engaging third-party security auditors and internal personnel to run automated security monitoring;

iv. Auditing, testing, and training their security personnel regarding any new or modified procedures;

v. Segmenting their user applications by, among other things, creating firewalls and access controls so that if one area is compromised, hackers cannot gain access to other portions of Defendants' systems, networks, and servers;

vi. Conducting regular database scanning and security checks; and

vii. Routinely and continually conducting internal training and education to inform Defendants' internal security personnel how to identify and contain a data breach when it occurs and what to do in response to a breach.

160. If an injunction is not issued, Plaintiff and the Class will suffer irreparable injury and will lack an adequate legal remedy to prevent another data breach or cybersecurity incident. This risk is real, immediate, and substantial. If another data breach or cybersecurity incident occurs with Defendants, Plaintiff and the Class will not have an adequate remedy at law because many of the resulting injuries are not readily quantifiable.

161. The hardship to Plaintiff and the Class if an injunction is not issued exceeds the hardship to Defendants if an injunction is issued. Plaintiff and the Class will likely be subjected to substantial, continued identity theft and other related damages if an injunction is not issued. On the other hand, the cost of Defendants' compliance with an injunction requiring reasonable prospective data security measures is relatively minimal, and Defendants have a pre-existing legal obligation to employ such measures.

162. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing a subsequent data breach or cybersecurity incident with Defendants, thus preventing future injury to Plaintiff and the Class and other persons whose PII and PHI would be further compromised.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of themselves and the Class set forth herein, respectfully requests that the Court order the following relief and enter judgment against Defendants as follows:

A. Certifying this action as a class action under Federal Rule of Civil Procedure 23 and appointing Plaintiff and his counsel to represent the Class;

B. Declaring that Defendants engaged in the illegal and wrongful conduct alleged herein;

C. Entering judgment for Plaintiff and the Class;

D. Granting permanent and appropriate injunctive relief to prohibit Defendants from continuing to engage in the unlawful or wrongful acts, omissions, and practices described herein and directing Defendants to adequately safeguard the PII and PHI of Plaintiff and the Class by implementing improved security controls;

E. Awarding compensatory, consequential, and general damages, including nominal damages as appropriate, as allowed by law in an amount to be determined at trial;

F. Awarding statutory or punitive damages and penalties as allowed by law in an amount to be determined at trial;

G. Ordering disgorgement and restitution of all earnings, profits, compensation, and benefits received by Defendants as a result of Defendants' unlawful acts, omissions, and practices;

H. Awarding to Plaintiff and Class Members the costs and disbursements of the action, along with reasonable attorneys' fees, costs, and expenses;

I. Awarding pre- and post-judgment interest at the maximum legal rate and all such other relief as it deems just and proper; and

J. Granting such further and other relief as may be just and proper.

DEMAND FOR JURY TRIAL

Plaintiff hereby demands a trial by jury for all claims and issues so triable.

Dated: July 8, 2024 By: */s/James C. Shah*

James C. Shah (S.B.N. 80337)
Alec J. Berin (S.B.N. 328071)
MILLER SHAH LLP
1845 Walnut Street, Suite 806
Philadelphia, PA 19103
Telephone: (866) 540-5505
Facsimile: (866) 300-7367
jcshah@millershah.com
ajberin@millershah.com

Amber L. Schubert
SCHUBERT JONCKHEER & KOLBE LLP
2001 Union St., Suite 200
San Francisco, CA 94123
Telephone: (415) 788-4220
Facsimile: (415) 788-0161
aschubert@sjk.law

Edward F. Haber
Ian J. McLoughlin
SHAPIRO HABER & URMY LLP
One Boston Place, Suite 2600
Boston, MA 02108
Telephone: (617) 439-3939
Facsimile: (617) 439-0134
ehaber@shulaw.com
imcloughlin@shulaw.com

Counsel for Plaintiff Theodore Tasangarinos and the Putative Class