IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF PENNSYLVANIA

JOHN HOLLIS, *individually and on behalf of all others similarly situated*, Plaintiff, v. CENCORA, INC. and THE LASH GROUP, LLC, Defendants.	Case No. 2:24-cv-2863 **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiff John Hollis, by and through his undersigned counsel, hereby files this Class Action Complaint, individually and on behalf of all others similarly situated, against Defendants Cencora, Inc. ("Cencora") and The Lash Group, LLC ("Lash Group") (collectively, "Defendants"). Plaintiff bases the following allegations upon information and belief, investigation of counsel, and his own personal knowledge.

NATURE OF THE ACTION

1. Plaintiff brings this action against Defendants for their failure to properly secure and safeguard individuals' personally identifying information ("PII") and protected health information ("PHI") including, *inter alia*, consumers' first names, last names, dates of birth, health diagnoses, medications, and prescriptions.

2. Businesses that handle PII and PHI owe a duty to the individuals to whom that data relates. This duty to protect PII and PHI arises because it is foreseeable that its exposure to unauthorized persons—especially to hackers with nefarious intentions—will result in harm to the affected individuals.

3. The harm resulting from a data privacy breach manifests in a number of ways, including identity theft and financial fraud, and the exposure of a person's PII or PHI through a

data breach ensures that such person will be at a substantially increased and certainly impending risk of identity theft crimes compared to the rest of the population, potentially for the rest of their lives. Mitigating that risk—to the extent it is even possible to do so—requires individuals to devote significant time and money to closely monitor their credit, financial accounts, health records, and email accounts, and take a number of additional prophylactic measures.

4. Cencora is a pharmaceutical giant that provides services related to drug distribution, specialty pharmacy, consulting, and clinical trial support.[1] Lash Group, a division of Cencora, specializes in patient support technologies.[2] Defendants work with pharmaceutical firms, healthcare providers, and pharmacies to offer drug distribution, patient support services, business analytics, and technology, and other services.

5. In order to provide these services to their clients, Defendants are entrusted consumer and patient PII and PHI. As Defendants are or should have been aware, this type of personal and sensitive data is highly targeted by hackers who seek to exploit that data for nefarious purposes. In the wrong hands, these types of sensitive data may be wielded to cause significant harm to the Class Members.

6. In turn, Defendants have a duty to secure, maintain, protect, and safeguard the PII and PHI with which they have been entrusted against unauthorized access and disclosure through reasonable and adequate data security measures.

[1] Bill Toulas, *Cencora Data Breach Exposes US Patient Info from 11 Drug Companies*, Bleeping Computer (May 25, 2024), https://www.bleepingcomputer.com/news/security/cencora-data-breach-exposes-us-patient-info-from-11-drug-companies/.

[2] The Lash Group, https://www.lashgroup.com/#:~:text=We%20pair%20advanced%20technologies%20with,every%20step%20of%20the%20way (last visited July 1, 2024).

7. Despite Defendants' duty to safeguard PII and PHI, Plaintiff's and Class Members' sensitive information was exposed to unauthorized third parties during a massive data breach following a February 2024 cyberattack (the "Data Breach").[3]

8. In the wake of the cyberattack, Defendants' clients, some of the largest pharmaceutical firms in the United States, have begun to notify affected individuals that their valuable PII and PHI—including their full names, addresses, health diagnoses, medications, and prescriptions—that was entrusted to Defendants was exposed and exfiltrated as a result of the Data Breach.[4]

9. While Cencora initially disclosed the Data Breach in a public filing in February 2024, it revealed very little information.[5] To date, it is still unknown just how many individuals' PII and PHI was implicated as a result of the Data Breach. Additionally, despite becoming aware of unauthorized access to its systems on February 21, 2024, Defendants did not begin notifying affected individuals until late May 2024.

---

[3] Toulas, *supra* note 1.

[4] *See* Novartis Submitted Breach Notification Sample (May 22, 2024), https://oag.ca.gov/ecrime/databreach/reports/sb24-585783; Bayer Submitted Breach Notification Sample (May 20, 2024), https://oag.ca.gov/ecrime/databreach/reports/sb24-585635; AbbVie Submitted Breach Notification Sample (May 21, 2024), https://oag.ca.gov/ecrime/databreach/reports/sb24-585726; Regeneron Submitted Breach Notification Sample (May 22, 2024), https://oag.ca.gov/ecrime/databreach/reports/sb24-585823; Genentech Submitted Breach Notification Sample (May 20, 2024), https://oag.ca.gov/ecrime/databreach/reports/sb24-585650; Incyte Submitted Breach Notification Sample (May 23, 2024), https://oag.ca.gov/ecrime/databreach/reports/sb24-585847; Sumitomo Pharma Submitted Breach Notification Sample (May 23, 2024), https://oag.ca.gov/ecrime/databreach/reports/sb24-585855; Acadia Submitted Breach Notification Sample (May 21, 2024), https://oag.ca.gov/ecrime/databreach/reports/sb24-585716; GlaxoSmithKline Submitted Breach Notification Sample (May 24, 2024), https://oag.ca.gov/ecrime/databreach/reports/sb24-585929; Endo Submitted Breach Notification Sample (May 24, 2024), https://oag.ca.gov/ecrime/databreach/reports/sb24-585914; Dendreon Submitted Breach Notification Sample (May 23, 2024), https://oag.ca.gov/ecrime/databreach/reports/sb24-585889.

[5] Cencora, Inc., *Form 8-K Current Report* (February 21, 2024), https://www.sec.gov/Archives/edgar/data/1140859/000110465924028288/tm247267d1_8k.htm.

10. As described herein, Plaintiff's and Class Members' PII and PHI is now in the hands of cybercriminals as a direct and proximate result of Defendants' failure to implement and follow basic security procedures.

11. As a direct and proximate result of Defendants' inadequate data security measures, and its breach of its duty to handle PII and PHI with reasonable care, Plaintiff's and Class Members' PII and PHI has been accessed by malicious threat actors and exposed to an untold number of unauthorized individuals.

12. Plaintiff and Class Members are now at a significantly increased and certainly impending risk of fraud, identity theft, misappropriation of health insurance benefits, intrusion of their health privacy, and similar forms of criminal mischief, risk which may last for the rest of their lives. Consequently, Plaintiff and Class Members must devote substantially more time, money, and energy to protect themselves, to the extent possible, from these crimes.

13. Plaintiff, on behalf of himself, and the Class as defined herein, brings claims for negligence, negligence *per se*, and declaratory judgment, seeking actual and putative damages, with attorneys' fees, costs, and expenses, and appropriate injunctive and declaratory relief.

14. To recover from Defendants for these harms, Plaintiff and the Class seek damages in an amount to be determined at trial, declaratory judgment, and injunctive relief requiring Defendants to: (1) investigate and disclose, expeditiously, the full nature of the Data Breach and the types of PII and PHI accessed, obtained, or exposed by the hackers; (2) implement improved data security practices to reasonably guard against future breaches of PII and PHI possessed by Defendants; and (3) provide, at Defendants' own expense, all impacted victims with lifetime identity protection services.

PARTIES

15. Plaintiff John Hollis is an adult, who at all relevant times, is and was a citizen of the State of Indiana.

16. Defendant Cencora, Inc. is a Delaware corporation with its principal place of business located at 1 West First Avenue, Conshohocken, Pennsylvania 19428.

17. Defendant The Lash Group LLC is a Delaware limited liability company with a principal place of business located at 1 West First Avenue, Conshohocken, Pennsylvania 19428. Upon information and belief, Lash Group's sole member is AmerisourceBergen Consulting Services, LLC, a Delaware limited liability company. AmerisourceBergen Consulting Services, LLC's sole member is AmerisourceBergen Drug Corporation, a Delaware corporation whose principal place of business is located at 1 West First Avenue, Conshohocken, Pennsylvania 19428. AmerisourceBergen Drug Corporation's sole shareholder in turn is Defendant Cencora, Inc. The Lash Group is a citizen of each State in which its member is a citizen. The Lash Group is therefore a citizen of the Commonwealth of Pennsylvania and the State of Delaware.

JURISDICTION AND VENUE

18. This Court has jurisdiction over this action pursuant to 28 U.S.C. § 1332(d)(2)(A), as modified by the Class Action Fairness Act of 2005, because Plaintiff and at least one member of the Class, as defined below, is a citizen of a different state than Defendants, there are more than 100 members of the Class, and the aggregate amount in controversy exceeds $5,000,000 exclusive of interests and costs.

19. This Court has personal jurisdiction over Defendants, as Defendants both maintain their principal place of business in Conshohocken, Pennsylvania, and, at all relevant times, Defendants have engaged in substantial business activities in Pennsylvania, regularly conduct business in Pennsylvania, and have sufficient minimum contacts in Pennsylvania.

20. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(b) because Defendants' principal place of business is in this District and a substantial part of the events, acts, and omissions giving rise to Plaintiff's claims occurred in this District

FACTUAL BACKGROUND

A. Defendants Collected and Stored Plaintiff's and Class Members' PII and PHI.

21. Cencora, formerly known as AmerisourceBergen, is a massive global pharmaceutical sourcing and distribution company that provides a wide range of pharmaceuticals, healthcare products, and related services to healthcare providers worldwide. Its clients include "acute care hospitals and health systems, independent and chain retail pharmacies, mail order pharmacies, medical clinics, long-term care and alternate site pharmacies, physician practices, medical and dialysis clinics, veterinarians, and other customers."[6]

22. Cencora proudly asserts that it is "one of the largest global pharmaceutical sourcing and distribution services companies." In 2023 alone, its annual revenue increased nearly 10%, totaling more than $262 million. [7] Cencora employs approximately 46,000 individuals, operates in fifty countries,[8] and handles around 20% of the pharmaceuticals sold and distributed throughout the United States.[9]

23. Lash Group, a subsidiary of Cencora, "designs and delivers patient access and adherence programs."[10]

---

[6] Cencora, *Form 10-K* (Nov. 1, 2023), https://investor.amerisourcebergen.com/files/doc_financials/2023/ar/Cencora-FY2023-10-K-Web-Posting.pdf.
[7] *Id.*
[8] *Id.*
[9] Zack Whittaker, *US Pharma Giant Cencora Says Americans' Health Information Stolen in Data Breach*, TechCrunch (May 24, 2024), https://techcrunch.com/2024/05/24/cencora-americans-health-data-stolen-breach-cyberattack/.
[10] *Our Network*, Lash Group, https://www.lashgroup.com/our-network (last visited July 1, 2024).

24. Together, Defendants ship nearly seven million products daily, have served fifteen million patients, and have risen to #11 on the Fortune 500 list.[11]

25. Together, Defendants work with pharmaceutical firms, healthcare providers, and pharmacies to offer drug distribution, patient support services, business analytics, and technology, and other services.

26. As a condition of providing these services, Defendants receive, create, and handle the PII and PHI of Plaintiff and Class Members.

27. Plaintiff and Class Members must directly or indirectly entrust Defendants with their sensitive and confidential PII and PHI in order to receive health care services, and in return reasonably expected that Defendants would safeguard their highly sensitive information and keep it confidential.

28. Due to the sensitivity of the PII and PHI that Defendants handle, Defendants are aware of their critical responsibility to safeguard this information—and, therefore, how devastating its theft is to individuals whose information has been stolen.

29. By obtaining, collecting, and storing Plaintiff's and Class Members' PII and PHI, Defendants assumed equitable and legal duties to safeguard and keep confidential Plaintiff's and Class Members' highly sensitive information, to only use this information for business purposes, and to only make authorized disclosures.

30. Despite the existence of these duties, Defendants failed to implement reasonable data security measures to protect the information with which it was entrusted, and ultimately allowed nefarious third-party hackers to compromise Plaintiff's and Class Members' PII and PHI.

[11] *Who We Are*, Cencora, https://www.cencora.com/who-we-are (last visited July 1, 2024); *Who We Are*, Lash Group, https://www.lashgroup.com/who-we-are (last visited July 1, 2024).

B. Defendants are Subject to HIPAA as Business Associates.

31. Upon information and belief, Defendants are Health Insurance Portability and Accountability Act ("HIPAA") covered business associates that provide services to various healthcare providers (*i.e.*, HIPAA "Covered Entities").[12]

32. As a regular and necessary part of their business, Defendants collect and maintain patients' highly sensitive PHI. Defendants are required under federal law to maintain the strictest confidentiality of the patients' PHI that it acquires, receives, and collects, and Defendants are further required to maintain sufficient safeguards to protect that PHI from being accessed by unauthorized third parties.

33. Due to their status as HIPAA-covered business associates, Defendants are required to enter into contracts with its Covered Entities to ensure that Defendants will implement adequate safeguards to prevent unauthorized use or disclosure of PHI, including by implementing requirements of the HIPAA Security Rule[13] and to report to the Covered Entities any unauthorized use or disclosure of PHI, including incidents that constitute breaches of unsecured PHI as in the case of the Data Breach complained of herein.

34. Indeed, both Defendants claim to maintain protected information in compliance with HIPAA requirements.[14]

---

[12] *See* 45 CFR § 160.103.

[13] The HIPAA Security Rule establishes national standards to protect individuals' electronic personal health information that is created, received, used, or maintained by a covered entity. The Security Rule requires appropriate administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of electronic protected health information. *See* 45 C.F.R. Part 160 and Part 164, Subparts A and C.

[14] *Form 10-K*, *supra* note 6; *Notice of Privacy Practices*, Lash Group (July 1, 2012), https://www.lashgroup.com/notice-of-privacy-practices.

35. Despite these assurances and Defendants' duty to safeguard Plaintiff's and Class Members' PII and PHI, Defendants employed inadequate data security measures to protect and secure the PII and PHI with which they were entrusted, resulting in the Data Breach and compromise of Plaintiff's and Class Members' PII and PHI stored within their computer networks.

C. Defendants Knew the Risks of Storing Valuable PII and PHI.

36. Defendants were well aware that the PII and PHI they collect is highly sensitive and of significant value to those who would use it for wrongful purposes.

37. Defendants also knew that a breach of their computer systems, and exposure of the information stored therein, would result in the increased risk of identity theft and fraud against the individuals whose PII and PHI was compromised, as well as intrusion into their highly private health information.

38. These risks are not theoretical; in recent years, numerous high-profile breaches have occurred at business such as Equifax, Facebook, Yahoo, Marriott, Anthem, and other healthcare partner and provider companies, including Managed Care of North America, OneTouchPoint, Inc., Shields Healthcare Group, Eye Care Leaders and Connexin Software, Inc., and Blackbaud.

39. PII has considerable value and constitutes an enticing and well-known target to hackers. Hackers easily can sell stolen data as there has been a "proliferation of open and anonymous cybercrime forums on the Dark Web that serve as a bustling marketplace for such commerce."[15] PHI, in addition to being of a highly personal and private nature, can be used for medical fraud and to submit false medical claims for reimbursement.

[15] Brian Krebs, *The Value of a Hacked Company*, Krebs on Security (July 14, 2016), http://krebsonsecurity.com/2016/07/the-value-of-a-hacked-company/.

40. The prevalence of data breaches and identity theft has increased dramatically in recent years, accompanied by a parallel and growing economic drain on individuals, businesses, and government entities in the U.S. In 2021, there were 4,145 publicly disclosed data breaches, exposing 22 billion records. The United States specifically saw a 10% increase in the total number of data breaches.[16]

41. In tandem with the increase in data breaches, the rate of identity theft complaints has also increased over the past few years. For instance, in 2017, 2.9 million people reported some form of identity fraud compared to 5.7 million people in 2021.[17]

42. The healthcare industry has become a prime target for threat actors: "High demand for patient information and often-outdated systems are among the nine reasons healthcare is now the biggest target for online attacks."[18] Indeed, "[t]he IT environments of healthcare organizations are often complex and difficult to secure. Devices and software continue to be used that have reached end-of-life, as upgrading is costly and often problematic. Many healthcare providers use software solutions that have been developed to work on specific – and now obsolete – operating systems and cannot be transferred to supported operating systems."[19]

43. Cybercriminals seek out PHI at a greater rate than other sources of personal information. Between 2009 and 2022, 5,150 healthcare data breaches of 500 or more individuals

---

[16] *Data Breach Report: 2021 Year End*, Risk Based Security (Feb. 4, 2022), https://www.riskbasedsecurity.com/2022/02/04/data-breach-report-2021-year-end.

[17] *Insurance Information Institute, Facts + Statistics: Identity theft and cybercrime*, Insurance Information Institute, https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime#Identity%20Theft%20And%20Fraud%20Reports,%202015-2019%20 (last visited July 1, 2024).

[18] *The healthcare industry is at risk*, SwivelSecure https://swivelsecure.com/solutions/healthcare/healthcare-is-the-biggest-target-for-cyberattacks/ (last visited July 1, 2024).

[19] Steve Alder, Editorial: *Why Do Criminals Target Medical Records*, HIPAA Journal (Oct. 14, 2022), https://www.hipaajournal.com/why-do-criminals-target-medical-records/#:~:text=Healthcare%20records%20are%20so%20valuable,credit%20cards%20in%20victims'%20names.

have been reported to Health and Human Services' Office of Civil Rights, resulting in the exposure or unauthorized disclosure of the information of 382,262,109 individuals—"[t]hat equates to more than 1.2x the population of the United States."[20]

44. Further, the rate of healthcare data breaches has been on the rise in recent years. "In 2018, healthcare data breaches of 500 or more records were being reported at a rate of around 1 per day. Fast forward 5 years and the rate has more than doubled. In 2022, an average of 1.94 healthcare data breaches of 500 or more records were reported each day."[21]

45. In a 2022 report, the healthcare compliance company Protenus found that there were 905 medical data breaches in 2021, leaving over 50 million patient records exposed for 700 of the 2021 incidents. This is an increase from the 758 medical data breaches that Protenus compiled in 2020.[22]

46. The healthcare sector suffered about 337 breaches in the first half of 2022 alone, according to Fortified Health Security's mid-year report released in July. The percentage of healthcare breaches attributed to malicious activity rose more than 5 percentage points in the first six months of 2022 to account for nearly 80 percent of all reported incidents.[23]

47. The breadth of data compromised in the Data Breach makes the information particularly valuable to thieves and leaves Plaintiff and Class Members especially vulnerable to identity theft, tax fraud, medical fraud, credit and bank fraud, and more.

---

[20] *Healthcare Data Breach Statistics*, HIPAA Journal, https://www.hipaajournal.com/healthcare-data-breach-statistics/ (last visited July 1, 2024).
[21] *Id.*
[22] *2022 Breach Barometer*, PROTENUS, https://www.protenus.com/breach-barometer-report (last visited July 1, 2024).
[23] Jill McKeon, *Health Sector Suffered 337 Healthcare Data Breaches in First Half of Year*, Cybersecurity News (July 19, 2022), https://healthitsecurity.com/news/health-sector-suffered-337-healthcare-data-breaches-in-first-half-of-year.

48. Medical Information—As indicated by Jim Trainor, former second in command at the FBI's cyber security division: "Medical records are a gold mine for criminals—they can access a patient's name, DOB, Social Security and insurance numbers, and even financial information all in one place. Credit cards can be, say, five dollars or more where PHI records can go from $20 say up to—we've even seen $60 or $70."[24] A complete identity theft kit that includes health insurance credentials may be worth up to $1,000 on the black market, whereas stolen payment card information sells for about $1.[25]

49. Indeed, medical records "are so valuable because they can be used to commit a multitude of crimes. Healthcare data can be used to impersonate patients to obtain expensive medical services, Medicare and Medicaid benefits, healthcare devices, and prescription medications. Healthcare records also contain the necessary information to allow fraudulent tax returns to be filed to obtain rebates."[26]

50. "In contrast to credit card numbers and other financial information, healthcare data has an incredibly long lifespan and can often be misused for long periods undetected. Credit card companies monitor for fraud and rapidly block cards and accounts if suspicious activity is detected, but misuse of healthcare data is harder to identify and can be misused in many ways before any malicious activity is detected. During that time, criminals can run up huge debts – far more than is usually possible with stolen credit card information."[27]

---

[24] *You Got It, They Want It: Criminals Targeting Your Private Healthcare Data*, *New Ponemon Study Shows*, IDX (May 14, 2015), https://www.idexpertscorp.com/knowledge-center/single/you-got-it-they-want-it-criminals-are-targeting-your-private-healthcare-dat.

[25] *Managing cyber risks in an interconnected world, Key findings from The Global State of Information Security® Survey 2015*, PriceWaterhouseCoopers, https://www.pwc.com/gx/en/consulting-services/information-security-survey/assets/the-global-state-of-information-security-survey-2015.pdf (last visited July 1, 2024).

[26] Alder, *supra* note 19.

[27] *Id.*

51. According to Experian:

> Having your records stolen in a healthcare data breach can be a prescription for financial disaster. If scam artists break into healthcare networks and grab your medical information, they can impersonate you to get medical services, use your data open credit accounts, break into your bank accounts, obtain drugs illegally, and even blackmail you with sensitive personal details.

52. Victims of healthcare data breaches may also find themselves being denied care, coverage, or reimbursement by their medical insurers, having their policies canceled or having to pay to reinstate their insurance, along with suffering damage to their credit ratings and scores. In the worst cases, they've been threatened with losing custody of their children, been charged with drug trafficking, found it hard to get hired for a job, or even been fired by their employers.[28]

53. Even if stolen, PII or PHI does not include financial or payment card account information, that does not mean there has been no harm, or that the breach does not cause a substantial risk of identity theft. Freshly stolen information can be used with success against victims in specifically targeted efforts to commit identity theft known as social engineering or spear phishing. In these forms of attack, the criminal uses the previously obtained PII and PHI about the individual, such as name, address, email address, and affiliations, to gain trust and increase the likelihood that a victim will be deceived into providing the criminal with additional information.

54. Based on the aforementioned cybercrime trends and the value of PII and PHI to cybercriminals, Defendants should have known the importance of safeguarding the PII and PHI with which they were entrusted, and of the foreseeable consequences if its data security systems were breached.

---

[28] Brian O'Connor, *Healthcare Data Breach: What to Know About them and What to Do After One*, EXPERIAN (June 14, 2018), https://www.experian.com/blogs/ask-experian/healthcare-data-breach-what-to-know-about-them-and-what-to-do-after-one/.

55. Defendants have publicly acknowledged the risk of a cyber-attack as well. In Cencora's most recently filed Annual Report, it noted the risk of cyber-attacks and data security incidents. As part of this detailed discussion, Cencora stated:

> Information security risks have generally increased in recent years because of the proliferation of cloud-based infrastructure and other services, new technologies, and the increased sophistication and activities of perpetrators of cyberattacks. Security incidents such as ransomware attacks are becoming increasingly prevalent and severe, as well as increasingly difficult to detect. These risks have increased with the growth of our business, including as we integrate the information systems of acquired businesses, such as Alliance Healthcare, into our enterprise.
>
> In addition, security incidents may disrupt our businesses and require that we expend substantial additional resources related to the security of information systems. We, and our third-party service providers, have experienced cyberattacks. For example, in March 2023, one of our foreign business units experienced a cybersecurity event that resulted in the unavailability of certain data stored on a standalone legacy information technology platform and disrupted operations of the Company's foreign business unit in that country. Although the prior incidents did not have a material impact on us, either individually or in the aggregate, similar incidents or events in the future may materially impact our business, reputation or financial results.
>
> Security breaches can also occur as a result of non-technical issues, including intentional or inadvertent actions by our employees, third-party service providers or their personnel or other parties.[29]

56. Defendants had actual and constructive knowledge of the value of PII and PHI to cybercriminals, the importance of safeguarding the PII and PHI with which they had been entrusted, and the foreseeable consequences of their systems were breached. Nonetheless, Defendants failed to take adequate cyber-security measures to prevent the Data Breach from occurring.

D. Defendants Breached their Duty to Protect Patient PII and PHI.

57. On February 27, 2024, Cencora filed notice with the Securities and Exchange Commission ("SEC") that it had discovered the Data Breach. The report reads:

[29] *Form 10-K*, *supra* note 6.

> On February 21, 2024, Cencora, Inc. (the "Company"), learned that data from its information systems had been exfiltrated, some of which may contain personal information. Upon initial detection of the unauthorized activity, the Company immediately took containment steps and commenced an investigation with the assistance of law enforcement, cybersecurity experts and external counsel.[30]

58. Approximately three months thereafter, Defendants finally began to send notice letters to affected individuals.[31] The notice letters were sent on Cencora letterhead by some of the largest pharmaceutical firms in the United States, and all attributed the exposure and exfiltration of PII and PHI to the Data Breach.[32]

59. The notice letters, all substantively identical, inform affected individuals that their PII and PHI (including, *inter alia*, consumers' first names, last names, dates of birth, health diagnoses, medications, and prescriptions) had been exfiltrated from Cencora's information systems in the Data Breach.[33]

60. Many details about the Data Breach are still unknown. Neither the notice letters nor any other public statements address the manner in which cybercriminals were able to access Defendants' systems, the identity of the hackers, whether a ransom was demanded and/or paid, or what safeguards have been put in place since the Data Breach.

61. Defendants are even refusing to report the number of individuals affected by the Data Breach; when asked by journalists, a Cencora spokesperson was "unwilling to say if the company has determined how many individuals are affected by the breach and how many individuals the company has notified to date."[34]

---

[30] *Form 8-K*, *supra* note 5.
[31] *See* Submitted Breach Notification Samples, *supra* note 4.
[32] *Id.*; Toulas, *supra* note 1.
[33] *See* Submitted Breach Notification Samples, *supra* note 4.
[34] Whittaker, *supra* note 9.

62. However, based on clients' of Defendants notifications to state Attorneys General, the Data Breach at a minimum, has impacted hundreds of thousands of individuals.[35]

63. Although many specific details about the Data Breach (including the above) are still unknown, it is evident that bad actors accessed Defendants' computer systems in an intentional attack designed to acquire consumers' valuable PII and PHI stored therein, and that the cybercriminals were successful in the attack.

64. As a result of the Data Breach, the PII and PHI of at minimum hundreds of thousands of individuals—including Plaintiff and Class Members—was accessed, viewed, exfiltrated, and is now in the hands of cybercriminals.

E. Defendants Failed to Comply with FTC Guidelines.

65. Defendants are prohibited by the Federal Trade Commission Act, 15 U.S.C. § 45 ("FTC Act") from engaging in "unfair or deceptive acts or practices in or affecting commerce." The Federal Trade Commission ("FTC") has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of the FTC Act.

66. The FTC has promulgated numerous guides for businesses that highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[36]

[35] Steve Alder, *More than a Dozen Pharmaceutical Companies Affected by Cencora Cyberattack*, HIPAA Journal (May 27, 2024), https://www.hipaajournal.com/cencora-cyberattack-data-breach/.
[36] *Start with Security: A Guide for Business*, Fed. Trade Comm'n, https://www.ftc.gov/business-guidance/resources/start-security-guide-business (last visited July 1, 2024).

67. In 2016, the FTC updated its publication titled Protecting Personal Information: A Guide for Business, which established cyber-security guidelines for businesses.[37] The guidelines state that:

a. Businesses should promptly dispose of personal identifiable information that is no longer needed, and retain sensitive data "only as long as you have a business reason to have it;

b. Businesses should encrypt sensitive personal information stored on computer networks so that it is unreadable even if hackers are able to gain access to the information;

c. Businesses should thoroughly understand the types of vulnerabilities on their network and how to address those vulnerabilities;

d. Businesses should install intrusion detection systems to promptly expose security breaches when they occur; and

e. Businesses should install monitoring mechanisms to watch for large troves of data being transmitted from their systems.

68. In another publication, the FTC recommended that companies not maintain PII longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.[38]

69. Notably, the FTC treats the failure to employ reasonable data security safeguards as an unfair act or practice prohibited by Section 5 of the FTC Act. Indeed, the FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer

[37] *See Protecting Personal Information: A Guide for Business*, Federal Trade Commission, October 2016, available at https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business (last visited July 1, 2024).
[38] *See Start with Security: A Guide for Business*, Federal Trade Commission, June 2015, available at https://www.ftc.gov/tips-advice/business-center/guidance/start-security-guide-business (last visited June 5, 2024).

data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the FTC Act. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

70. Upon information and belief, Defendants failed to properly implement one or more of the basic data security practices recommended by the FTC. Defendants' failure to employ reasonable and appropriate data security measures to protect against unauthorized access to patients' PII and/or PHI constitutes an unfair act of practice prohibited by Section 5 of the FTC Act.

71. Similarly, the U.S. Government's National Institute of Standards and Technology ("NIST") provides a comprehensive cybersecurity framework that companies of any size can use to evaluate and improve their information security controls.[39]

72. NIST publications include substantive recommendations and procedural guidance pertaining to a broad set of cybersecurity topics including risk assessments, risk management strategies, access controls, training, data security controls, network monitoring, breach detection, and incident response.[40] Upon information and belief, Defendants failed to adhere to the NIST guidance.

73. Further, cybersecurity experts have identified various best practices that should be implemented by entities in the healthcare security, including implementing the following measures:

[39] *See Framework for Improving Critical Infrastructure Cybersecurity*, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (April 16, 2018), Appendix A, Table 2, available at https://nvlpubs.nist.gov/nistpubs/cswp/nist.cswp.04162018.pdf.
[40] *Id.* at Table 2 pg. 26-43.

a. Email protection systems and controls;

b. Endpoint protection systems;

c. Identify all users and audit their access to data, application, systems, and endpoints;

d. Data protection and loss prevention measures;

e. IT asset management;

f. Network management;

g. Vulnerability management;

h. Security operations center & incident response; and

i. Cybersecurity oversight and governance policies, procedures, and processes.[41]

74. Upon information and belief, Defendants' failure to protect massive amounts of PII is a result of their failure to adopt reasonable safeguards as required by the FTC guidelines, NIST guidance, and industry best practices.

75. Defendants were well aware of their obligations to use reasonable measures to protect patients' PII and PHI. Defendants also knew they were a target for hackers, as discussed above. Despite understanding the risks and consequences of inadequate data security, Defendants nevertheless failed to comply with its data security obligations.

F. Defendants are Obligated Under HIPAA to Safeguard Patient PHI.

76. As discussed above, Defendants are required by HIPAA, 42 U.S.C. § 1302d, *et seq*. to safeguard patient PHI.

[41] *HICP's 10 Mitigating Practices*, HHS, https://405d.hhs.gov/best-practices (last visited July 1, 2024).

77. HIPAA requires "compl[iance] with the applicable standards, implementation specifications, and requirements" of HIPAA "with respect to electronic protected health information." 45 C.F.R. § 164.302.

78. Under 45 C.F.R. § 160.103, HIPAA defines "protected health information" or PHI as "individually identifiable health information" that is "transmitted by electronic media; maintained in electronic media; or transmitted or maintained in any other form or medium."

79. Under 45 C.F.R. § 160.103, HIPAA defines "individually identifiable health information" as "a subset of health information, including demographic information collected from an individual" that is (1) "created or received by a health care provider;" (2)"[r]elates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual;" and (3) either "(i) identifies the individual; or (ii) with respect to which there is a reasonable basis to believe the information can be used to identify the individual."

80. HIPAA requires Defendants to: (a) ensure the confidentiality, integrity, and availability of all electronic PHI they create, receive, maintain, or transmit; (b) identify and protect against reasonably anticipated threats to the security or integrity of the electronic PHI; (c) protect against reasonably anticipated, impermissible uses, or disclosures of the PHI; and (d) ensure compliance by their workforce to satisfy HIPAA's security requirements. 45 C.F.R. § 164.102, *et seq*.

81. HHS further recommends the following data security measures that regulated entities—such as Defendants—should implement to protect against some of the more common, and often successful, cyber-attack techniques:

a. Regulated entities should implement security awareness and training for all workforce members and that the training programs should be ongoing, and

evolving to be flexible to educate the workforce on new and current cybersecurity treats and how to respond;

b. Regulated entities should implement technologies that examine and verify that received emails do not originate from known malicious site, scan web links or attachments included in emails for potential threats, and impeded or deny the introduction of malware that may attempt to access PHI;

c. Regulated entities should mitigate known data security vulnerabilities by patching or upgrading vulnerable technology infrastructure, by upgrading or replacing obsolete and/or unsupported applications and devices, or by implementing safeguards to mitigate known vulnerabilities until an upgrade or replacement can occur;

d. Regulated entities should implement security management processes to prevent, detect, contain, and correct security violations, including conducting risk assessments to identify potential risks and vulnerabilities to the confidentiality, integrity, and availability of PHI; and

e. Regulated entities should implement strong cyber security practices by requiring strong passwords rules and multifactor identification.[42]

82. Upon information and belief, Defendants failed to implement one or more of the recommended data security measures.

83. While HIPAA permits healthcare providers and their business associates to disclose PHI to third parties under certain circumstances, HIPAA does not permit Covered Entities to disclose PHI to cybercriminals, nor did Plaintiff or the Class Members consent to the disclosure of their PHI to cybercriminals.

84. As such, Defendants are required under HIPAA to maintain the strictest confidentiality of Plaintiff's and Class Members' PHI that they acquire, receive, and collect, and Defendants are further required to maintain sufficient safeguards to protect that information from being accessed by unauthorized third parties.

[42] *OCR Quarter 1 2022 Cybersecurity Newsletter*, U.S. Dept't of Health & Human Services (Mar. 17, 2023), https://www.hhs.gov/hipaa/for-professionals/security/guidance/cybersecurity-newsletter-first-quarter-2022/index.html.

85. Given the application of HIPAA to Defendants, and that Plaintiff and Class Members directly or indirectly entrusted their PHI to Defendants in order to receive healthcare services, Plaintiff and Class Members reasonably expected that Defendants would safeguard their highly sensitive information and keep their PHI confidential.

G. Plaintiff and Class Members Have Suffered Damages.

86. For the reasons mentioned above, Defendants' conduct, which allowed the Data Breach to occur, caused Plaintiff and Class Members to suffer significant harm in several ways, including substantial and imminent risk of identity theft and fraud. Plaintiff and Class Members must immediately devote time, energy, and money to: (1) closely monitor their medical statements, bills, records, and credit and financial accounts; (2) change login and password information on any sensitive account even more frequently than they already do; (3) more carefully screen and scrutinize phone calls, emails, and other communications to ensure that they are not being targeted in a social engineering, spear phishing, or extortion attacks; and (4) search for suitable identity theft protection and credit monitoring services, and pay to procure them.

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

88. As a result of Defendants' failures, Plaintiff and Class Members face an increased risk of identity theft, phishing attacks, and related cybercrimes because of the Data Breach. Those impacted are under heightened and prolonged anxiety and fear, as they will be at risk of falling victim to cybercrimes for years to come.

89. With respect to healthcare breaches, another study found "the majority [70 percent] of data impacted by healthcare breaches could be leveraged by hackers to commit fraud or identity theft."[43]

90. "Actors buying and selling PII and PHI from healthcare institutions and providers in underground marketplaces is very common and will almost certainly remain so due to this data's utility in a wide variety of malicious activity ranging from identity theft and financial fraud to crafting of bespoke phishing lures."[44]

91. Indeed, PII and PHI are valuable commodities to identity thieves and once they have been compromised, criminals will use them and trade the information on the cyber black market for years thereafter. All-inclusive health insurance dossiers containing sensitive health insurance information, names, addresses, telephone numbers, email addresses, Social Security Numbers, and bank account information, complete with account routing numbers can fetch up to $1,200 to $1,300 each on the black market.[45] According to a report released by the FBI's cyber division, criminals can sell healthcare records for 50 times the price of stolen Social Security Numbers or credit card numbers.[46]

---

[43] Jessica David, *70% of Data Involved in Healthcare Breaches Increases Risk of Fraud*, HEALTHITSECURITY, https://healthitsecurity.com/news/70-of-data-involved-in-healthcare-breaches-increases-risk-of-fraud (last visited July 1, 2024).

[44] *Id.*

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

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

92. The reality is that cybercriminals seek nefarious outcomes from a data breach and "stolen health data can be used to carry out a variety of crimes."[47]

93. Health information, in particular, is likely to be used in detrimental ways, by leveraging sensitive personal health details and diagnoses to extort or coerce someone, and serious and long-term identity theft.[48]

94. "Medical identity theft is a great concern not only because of its rapid growth rate, but because it is the most expensive and time consuming to resolve of all types of identity theft. Additionally, medical identity theft is very difficult to detect which makes this form of fraud extremely dangerous."[49]

95. Plaintiff and Class Members are also at a continued risk because their information remains in Defendants' systems, which have already been shown to be susceptible to compromise and attack and is subject to further attack so long as Defendants fail to undertake the necessary and appropriate security and training measures to protect its patients' PII and PHI.

96. Plaintiff and Class Members have suffered emotional distress as a result of the Data Breach, the increased risk of identity theft and financial fraud, and the unauthorized exposure of their private medical information to strangers.

H. Plaintiff's Experience.

97. Defendants were entrusted with Plaintiff's PII and PHI to facilitate access to their one of their client's patient support programs. In requesting and maintaining Plaintiff's PII and

---

[47] Andrew Steger, *What Happens to Stolen Healthcare Data?*, HEALTHTECH, (Oct. 30, 2019), https://healthtechmagazine.net/article/2019/10/what-happens-stolen-healthcare-data-perfcon.
[48] *Id.*
[49] *The Potential Damages and Consequences of Medical Identity theft and Healthcare Data Breaches*, EXPERIAN, https://www.experian.com/assets/data-breach/white-papers/consequences-medical-id-theft-healthcare.pdf (last visited July 1, 2024).

PHI, Defendants undertook a duty to act reasonably in its handling of Plaintiff's PII and PHI. Defendants, however, did not take reasonable care of Plaintiff's PII and PHI, leading to its exposure and compromise as direct and proximate result of Defendants' inadequate data security measures.

98. Plaintiff received a Data Breach Notification Letter from Defendants informing him that his PII and PHI that he directly and/or indirectly provided to Defendants was compromised in the Data Breach. The letter put the onus on Plaintiff to protect his PII and PHI by encouraging Plaintiff to remain vigilant.

99. Since the occurrence of the Data Breach, Plaintiff has been required to spend his valuable time and effort taking steps to mitigate the use of his PII and PHI, including changing his passwords to his various accounts, monitoring his accounts, and researching the Data Breach.

100. Plaintiff has suffered actual injury from having his PII and PHI exposed and/or stolen as a result of the Data Breach, including: (a) mitigation efforts to prevent the misuse of his PII an PHI; (b) damages to and diminution of the value of his PII and PHI, a form of intangible property that loses value when it falls into the hands of criminals who are using that information for fraud or publishing the information for sale on the dark web; and (c) loss of privacy.

101. In addition, knowing that hackers accessed and likely exfiltrated his PII and PHI and this information likely has been and will be used in the future for identity theft, fraud, and other nefarious purposes has caused Plaintiff to experience significant frustration, anxiety, worry, stress, and fear.

CLASS ACTION ALLEGATIONS

102. Plaintiff brings this Class Action on behalf of himself and all other similarly situated individuals pursuant to Rule 23 of the Federal Rules of Civil Procedure.

103. Plaintiff seeks to represent the following Class of persons defined as follows:

> All individuals in the United States whose PII and/or PHI was compromised as a result of the Data Breach of Cencora's systems detected on or about February 21, 2024.

104. Excluded from the Class are Defendants, their subsidiaries and affiliates, officers and directors, any entities in which Defendants have a controlling interest, the legal representative, heirs, successors, or assigns of any such excluded party, the judicial officer(s) to whom this action is assigned, and the members of their immediate families.

105. This proposed class definition is based on the information available to Plaintiff at this time. Plaintiff may modify the class definition in an amended pleading or when he moves for class certification, as necessary to account for any newly learned or changed facts as the situation develops and discovery gets underway.

106. **Numerosity:** The members of the Class are so numerous that the joinder of all members is impractical. Plaintiff is informed and believes, and thereon alleges, that there are at least hundreds of thousands of members of the Class described above. The exact size of the Class and the identities of the individual members are identifiable through Defendants' records, including but not limited to the files implicated in the Data Breach, but based on public information, the Class includes hundreds of thousands of individuals.

107. **Commonality:** This action involved questions of law and fact common to the Class. Such common questions include but are not limited to:

a. Whether Defendants had a duty to protect the PII and PHI of Plaintiff and Class Members;

b. Whether Defendants were negligent in collecting and storing Plaintiff's and Class Members' PII and PHI, and breached its duties thereby;

c. Whether Plaintiff and Class Members are entitled to damages as a result of Defendants' wrongful conduct; and

d. Whether Plaintiff and Class Members are entitled to restitution as a result of Defendants' wrongful conduct.

108. **Typicality:** Plaintiff's claims are typical of the claims of Class Members. Plaintiff's and Class Members' claims are based on the same legal theories and arise from the same unlawful and willful conduct. Plaintiff and Class Members each had their PII and PHI exposed and/or accessed by an unauthorized third party.

109. **Adequacy:** Plaintiff is an adequate representative of the Class. Plaintiff will fairly, adequately, and vigorously represent and protect the interests of the Class Members and has no interests antagonistic to the Class Members. In addition, Plaintiff has retained counsel who are competent and experienced in the prosecution of class action litigation. The claims of Plaintiff and the Class Members are substantially identical as explained above.

110. **Superiority:** This class action is appropriate for certification because class proceedings are superior to other available methods for the fair and efficient adjudication of this controversy and joinder of all Class members is impracticable. This proposed class action presents fewer management difficulties than individual litigation, and provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single court. Class treatment will create economies of time, effort, and expense, and promote uniform decision-making.

111. **Predominance:** Common questions of law and fact predominate over any questions affecting only individual Class Members. Similar or identical violations, business practices, and injuries are involved. Individual questions, if any, pale by comparison, in both quality and quantity, to the numerous common questions that dominate this action. For example, Defendants' liability and the fact of damages is common to Plaintiff and each member of the Class. If Defendants breached their duty to Plaintiff and Class Members, then Plaintiff and each Class member suffered damages by that conduct.

112. **Injunctive Relief:** Defendants have acted and/or refused to act on grounds that generally apply to the Class making injunctive and/or declaratory relief appropriate with respect to the Class under Fed. R. Civ. P. 23(b)(2).

113. **Ascertainability:** Class Members are ascertainable. Class membership is defined using objective criteria, and Class Members may be readily identified through Defendants' books and records.

FIRST CAUSE OF ACTION
NEGLIGENCE
(On Behalf of Plaintiff and the Class Against All Defendants)

114. Plaintiff restates and realleges the allegations contained in every preceding paragraph as if fully set forth herein.

115. Defendants owed a duty under common law to Plaintiff and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting their PII and PHI in Defendants' possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons.

116. Specifically, this duty included, among other things: (a) designing, maintaining, and testing Defendants' security systems to ensure that Plaintiff's and Class Members' PII PHI in Defendants' possession was adequately secured and protected; (b) implementing processes that would detect a breach of their security systems in a timely manner; (c) timely acting upon warnings and alerts, including those generated by their own security systems, regarding intrusions to their networks; and (d) maintaining data security measures consistent with industry standards.

117. Defendant's duty to use reasonable care arose from several sources, including but not limited to those described below.

118. Defendants owed a common law duty to Plaintiff and Class Members to implement reasonable data security measures because it was foreseeable that hackers would target

Defendants' data systems, software, and servers containing Plaintiff's and the Class's sensitive data and that, should a breach occur, Plaintiff and Class Members would be harmed. Defendants alone controlled their technology, infrastructure, and cybersecurity. They further knew or should have known that if hackers breached their data systems, they would extract sensitive data and inflict injury upon Plaintiff and Class Members. Furthermore, Defendants knew or should have known that if hackers accessed the sensitive data, the responsibility for remediating and mitigating the consequences of the breach would largely fall on individual persons whose data was impacted and stolen. Therefore, the Data Breach, and the harm it caused Plaintiff and Class Members, was the foreseeable consequence of Defendants' unsecure, unreasonable data security measures.

119. Defendants breached the duties owed to Plaintiff and Class Members and thus were negligent. Defendants breached these duties by, among other things: (a) mismanaging their systems and failing to identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that resulted in the unauthorized access and compromise of PII and PHI; (b) mishandling their data security by failing to assess the sufficiency of its safeguards in place to control these risks; (c) failing to design and implement information safeguards to control these risks; (d) failing to adequately test and monitor the effectiveness of the safeguards, key controls, systems, and procedures; (e) failing to evaluate and adjust their information security program in light of the circumstances alleged herein; (f) failing to detect the breach at the time it began or within a reasonable time thereafter; and (g) failing to adequately train and supervise employees and third party vendors with access or credentials to systems and databases containing sensitive PII and PHI.

120. But for Defendants' wrongful and negligent breach of their duties owed to Plaintiff and Class Members, their PII and PHI would not have been accessed and exfiltrated by cybercriminals.

121. As a direct and proximate result of Defendants' negligence, Plaintiff and Class Members have suffered injuries including:

a. Theft of their PII and PHI;

b. Costs associated with requesting credit freezes;

c. Costs associated with the detection and prevention of identity theft;

d. Costs associated with purchasing credit monitoring and identity theft protection services;

e. Lowered credit scores resulting from credit inquiries following fraudulent activities;

f. Costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Data Breach;

g. The imminent and certainly impending injury flowing from potential fraud and identity theft posed by their PII and PHI being placed in the hands of criminals;

h. Damages to and diminution in value of their PII and PHI entrusted to Defendants with the mutual understanding that Defendants would safeguard Plaintiff's and Class Members' data against theft and not allow access and misuse of their data by others; and

i. Continued risk of exposure to hackers and thieves of their PII and PHI, which remains in Defendants' possession and is subject to further breaches so long as Defendants fail to undertake appropriate and adequate measures to protect Plaintiff and Class Members.

122. As a direct and proximate result of Defendants' negligence, Plaintiff and Class Members are entitled to damages, including compensatory, punitive, and/or nominal damages, in an amount to be proven at trial.

SECOND CAUSE OF ACTION
NEGLIGENCE PER SE
(On Behalf of Plaintiff and the Class Against All Defendants)

123. Plaintiff restates and realleges the allegations contained in every preceding paragraph as if fully set forth herein.

124. Pursuant to Section 5 of the FTC Act, Defendants had a duty to provide fair and adequate computer systems and data security to safeguard the PII and/or PHI of Plaintiff and Class Members.

125. Defendants breached their duties to Plaintiff and Class Members under Section 5 of FTC Act by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' PII and/or PHI. Specifically, Defendants breached their duties by failing to employ industry-standard cybersecurity measures in order to comply with Section 5 of the FTC Act, including but not limited to proper segregation, access controls, password protection, encryption, intrusion detection, secure destruction of unnecessary data, and penetration testing.

126. 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 entities such as

Defendants or failing to use reasonable measures to protect PII and PHI. Various FTC publications and orders also form the basis of Defendants' duty.

127. It was reasonably foreseeable, particularly given the growing number of data breaches of PII and/or PHI within the healthcare industry, that the failure to reasonably protect and secure Plaintiff's and Class Members' PII and/or PHI in compliance with applicable laws would result in an unauthorized third-party gaining access to Defendants' networks, databases, and computers that stored Plaintiff's and Class Members' unencrypted PII and/or PHI.

128. Plaintiff and Class Members are within the class of persons that Section 5 of the FTC Act is intended to protect.

129. Moreover, the harm that has occurred is the type of harm that the FTC Act was intended to guard against. Indeed, the FTC has pursued over fifty enforcement actions against businesses which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm suffered by Plaintiff and Class Members.

130. Defendants' violation of Section 5 of the FTC Act constitutes negligence *per se.*

131. Furthermore, Defendants are Covered Entities under HIPAA, which sets minimum federal standards for privacy and security of PHI. Pursuant to HIPAA, 42 U.S.C. § 1302d, *et. seq.*, and its implementing regulations, Defendants had a duty to implement and maintain reasonable and appropriate administrative, technical, and physical safeguards to protect Plaintiff's and the Class members' electronic PHI.

132. Defendants violated HIPAA by actively disclosing Plaintiff's and the Class Members' electronic PHI; and by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' PHI.

133. Plaintiff and Class Members are patients within the class of persons HIPAA was intended to protect, as they are patients of Defendants' healthcare clients.

134. Moreover, the harm that has occurred is the type of harm that the HIPAA was intended to guard against.

135. Defendants' violation of HIPAA constitutes negligence *per se*.

136. As a direct and proximate result of Defendants' negligence *per se*, Plaintiff and Class Members have suffered injuries, including those identified above in paragraph 121.

137. As a direct and proximate result of Defendants' negligence, Plaintiff and Class Members have been injured as described herein, and are entitled to damages, including compensatory, punitive, and nominal damages, in an amount to be proven at trial.

THIRD CAUSE OF ACTION
DECLARATORY JUDGMENT
(On Behalf of Plaintiff and the Class Against All Defendants)

138. Plaintiff restates and realleges the allegations contained in every preceding paragraph as if fully set forth herein.

139. 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 grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal and state statutes described in this Class Action Complaint.

140. 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 continues to suffer injury as a result of the compromise

of his PII and PHI and remains at imminent risk that further compromises of his PII and/or PHI will occur in the future.

141. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring that, among other things:

a. Defendants owed a legal duty to secure patients' PII and PHI under the common law, Section 5 of the FTC Act, and HIPAA; and

b. Defendants breached and continues to breach this legal duty by failing to employ reasonable measures to secure patients' PII and PHI.

142. This Court also should issue corresponding prospective injunctive relief requiring Defendants to employ adequate security protocols consistent with law and industry standards to protect Plaintiff's and Class Members' PII and PHI.

143. If an injunction is not issued, Plaintiff and Class Members will suffer irreparable injury, and lack an adequate legal remedy, in the event of another data breach of any of Defendants' systems. The risk of another such breach is real, immediate, and substantial. If another breach of any of Defendants' systems occurs, Plaintiff will not have an adequate remedy at law because many of the resulting injuries are not readily quantified, and they will be forced to bring multiple lawsuits to rectify the same conduct.

144. The hardship to Plaintiff and Class Members if an injunction is not issued exceeds the hardship to Defendants if an injunction is issued. Plaintiff and Class Members will likely be subjected to substantial identity theft and other damage. On the other hand, the cost to Defendants of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Defendants have a pre-existing legal obligation to employ such measures.

145. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach of

Defendants' systems, thus eliminating the additional injuries that would result to Plaintiff, Class Members, and patients whose confidential information would be further compromised.

DEMAND FOR JURY TRIAL

Please take notice that Plaintiff demands a trial by jury as to all issues so triable in this action.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of himself and all others similarly situated, prays for relief as follows:

1. For an order certifying the Class under Rule 23 of the Federal Rules of Civil Procedure and naming Plaintiff as representative of the Class and Plaintiff's attorneys as Class Counsel to represent the Class;

2. For an order finding in favor of Plaintiff and the Class on all counts asserted herein;

3. For compensatory damages on behalf of Plaintiff and the Class;

4. For punitive damages on behalf of Plaintiff and the Class;

5. For an order of restitution and all other forms of equitable monetary relief;

6. Declaratory and injunctive relief as described herein;

7. For disgorgement and/or restitution as the Court deems appropriate, just, and proper;

8. Awarding Plaintiff reasonable attorneys' fees, costs, and expenses;

9. Awarding pre- and post-judgment interest on any amounts awarded;

10. For reimbursement for all costs and expenses incurred in connection with the prosecution of these claims; and

11. Awarding of such other and further relief as may be just and proper.

Dated: July 1, 2024

Respectfully submitted,

/s/ Gary F. Lynch
Gary F. Lynch (PA ID No. 56887)
Patrick D. Donathen (PA ID No. 330416)
LYNCH CARPENTER LLP
1133 Penn Avenue, 5th Floor
Pittsburgh, PA 15222
T: (412) 322-9243
gary@lcllp.com
patrick@lcllp.com

Brian C. Gudmundson*
ZIMMERMAN REED LLP
1100 IDS Center
80 South 8th Street
Minneapolis, MN 55402
T: (612)341-0400
brian.gudmundson@zimmreed.com

**pro hac vice forthcoming*

Attorneys for Plaintiff and the Proposed Class