

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

IVERY JOHNSON, individually and on
behalf of all others similarly situated,

Plaintiff,

v.

CENCORA, INC. and THE LASH GROUP,
LLC,

Defendants.

Case No. 2:24-cv-02227

CLASS ACTION

JURY TRIAL DEMANDED

CLASS ACTION COMPLAINT

Plaintiff Ivery Johnson (“Plaintiff”) brings this Class Action Complaint against Cencora, Inc. (“Cencora”) and the Lash Group, LLC (“Lash Group”) (together “Defendants”), individually and on behalf of all others similarly situated (“Class Members”), and alleges, upon personal knowledge as to his own actions and their counsels’ investigations, and upon information and good faith belief as to all other matters, as follows:

INTRODUCTION

1. Plaintiff brings this class action lawsuit against Defendants for their failure to properly secure and to safeguard the personally identifiable information and personal health information (“PII” and “PHI”, collectively “Private Information”) for half a million people.¹

2. On February 21, 2024, Cencora “learned that data from its information systems had been exfiltrated, some of which may contain personal information” by an unauthorized third-party

¹ *US drug maker Cencora says Americans’ health information stolen in data breach*, TechCrunch (May 24, 2024), available: <https://techcrunch.com/2024/05/24/cencora-americans-health-data-stolen-breach-cyberattack/#:~:text=According%20to%20the%20public%20data,learning%20of%20the%20data%20breach.>

(“the Data Breach”).² Upon learning of the “unauthorized activity”, Cencora commenced an investigation with the assistance of, *inter alia*, cybersecurity experts. *Id.* Following an investigation of the breach, Cencora determined that the incident compromised Private Information of individuals taking part in the Bristol Myers Squibb Patient Assistance Foundation, including their names, addresses, dates of birth, health diagnoses, medications, and prescriptions.

3. On February 27, 2024, Cencora filed an 8-K with the SEC (“SEC Filing” in which it disclosed:

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.

As of the date of this filing, the incident has not had a material impact on the Company’s operations, and its information systems continue to be operational. The Company has not yet determined whether the incident is reasonably likely to materially impact the Company’s financial condition or results of operations.³

4. Cencora, in its SEC Filing, acknowledges that Plaintiff’s and Class Members’ PII was unlawfully accessed and exfiltrated.

5. Despite announcing the Data Breach at the end of February, Cencora did not begin sending notice out to impacted individuals until late May.

6. Cencora has not yet disclosed details about the nature of the attack, what types of PII was compromised, or the number of individuals impacted.

7. Plaintiff brings this class action lawsuit on behalf of those similarly situated to

² <https://investor.amerisourcebergen.com/financials/sec-filings/default.aspx> (last visited Feb. 29, 2024) (“SEC Filing”).

³ *Id.*

address Cencora's inadequate safeguarding of Class Members' Private Information that it collected and maintained, and for failing to provide adequate notice to Plaintiff and Class Members.

PARTIES

A. Plaintiff Ivery Johnson

8. Plaintiff Ivery Johnson at all relevant times was and is a resident and citizen of North Ridgeville, Ohio.

9. Plaintiff Johnson's Private Information was in the possession and control of Defendants at the time of the Breach.

10. On or around May 17, 2024, Defendants notified Plaintiff Johnson that the Defendants' network had been accessed and Plaintiff's Private Information may have been involved in the Data Breach.

11. As a result of the Data Breach, Plaintiff Johnson spent time dealing with the consequences of the Data Breach, which includes time spent verifying the legitimacy of the Notice of Data Breach, and will now need to dedicate time to self-monitor his accounts and credit reports to ensure no fraudulent activity has occurred.

12. Even with the best response, the harm caused to Plaintiff Johnson cannot be undone.

13. Defendants admits that Plaintiff Johnson's Private Information was exfiltrated by criminal third-parties. Thus, Plaintiff Johnson's and Class Members' information is already being misused by cybercriminals.

14. Plaintiff Johnson has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from his Private Information being placed in the hands of unauthorized third parties and possibly criminals.

B. Defendant Cencora, Inc.

15. Defendant Cencora, Inc. is a company (formed in Delaware) with its principal place of business located at 1 West First Avenue, Conshohocken, PA 19428-1800.⁴ Cencora is a pharmaceutical services company that provides distribution solutions for doctor's offices, pharmacies, and animal healthcare.⁵

C. Defendant the Lash Group, LLC

16. Defendant the Lash Group, LLC is a company with its principal place of business located at 1 West 1st Avenue, Conshohocken, PA 19428-1800. 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, pharmacies, and other healthcare providers.⁶

17. The true names and capacities of persons or entities, whether individual, corporate, associate, or otherwise, who may be responsible for some of the claims alleged herein are currently unknown to Plaintiff. Plaintiff will seek leave of court to amend this complaint to reflect the true names and capacities of such other responsible parties when their identities become known.

18. All of Plaintiff's claims stated herein are asserted against Defendants and any of its owners, predecessors, successors, subsidiaries, agents and/or assigns.

JURISDICTION & VENUE

19. This Court has subject matter jurisdiction over this action further to the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2) because: (i) the amount in controversy exceeds \$5

⁴ *Id.*

⁵ <https://www.bleepingcomputer.com/news/security/pharmaceutical-giant-Cencora-says-data-was-stolen-in-a-cyberattack/amp/> (last visited Feb. 29, 2024)

⁶ <https://www.lashgroup.com/> (last visited May 24, 2024)

million, exclusive of interest and costs; (ii) the number of class members exceeds 100 and (iii) minimal diversity exists because many class members, including Plaintiff Johnson has different citizenship from Defendants.

20. This Court has personal jurisdiction over Defendant because it operates and is headquartered in this District and conducts substantial business in this District.

21. Venue is proper in this Court pursuant to 28 U.S.C. § 1331(a)(1) because a substantial part of the events giving rise to this action occurred in this District. Moreover, Defendant is based in this District, maintains Plaintiff's and Class Members' PII in this District, and has caused harm to Plaintiff and Class Members in this District.

FACTUAL ALLEGATIONS

Defendant's Business

22. Cencora is a Pennsylvania-based pharmaceutical services company that provides distribution solutions for doctor's offices, pharmacies, and animal healthcare.

23. Cencora, known as AmeriSourceBergen until 2023, handles around 20% of the pharmaceuticals sold and distributed throughout the United States.

24. As a condition of providing services, Cencora requires its clients to entrust it with their PII.

25. Upon information and belief, Cencora collects and maintains the Private Information of its clients, including but not limited to their:

- name,
- address,
- phone number and email address;
- date of birth;
- demographic information;
- information relating to individual medical history;
- information concerning an individual's doctor, nurse, or other medical providers;

- medication information;
- health insurance information;
- photo identification; and
- other information that Cencora may deem necessary to provide its services.

26. Because of the highly sensitive and personal nature of the information Cencora acquires and stores with respect to its clients, Plaintiff and Class Members reasonably expect that Cencora will, among other things: keep their Private Information confidential; comply with industry standards related to data security and Private Information; inform them of legal duties and comply with all federal and state laws protecting their Private Information; only use and release their Private Information for reasons that relate to providing services; and provide adequate notice to them if their Private Information is disclosed without authorization.

27. Plaintiff and Class Members entrusted Cencora with their Private Information but, contrary to Cencora's duties, promises, and the reasonable expectations of Plaintiff and Class Members, Cencora implemented substandard data security practices and failed to adhere to industry standard practices. Not only did Cencora maintain inadequate security to protect its systems from infiltration by cybercriminals, but it waited nearly three months to notify impacted individuals about the Data Breach.

The Data Breach

28. According to the SEC Filing made by Cencora, on February 21, 2024, Cencora learned that it was subject to a cybersecurity attack, but did not reveal when the attack occurred.

29. Cencora discovered that the Data Breach may have impacted Private Information stored in its systems and encrypted files.

30. In response, Cencora stated that “[u]pon 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.”⁷

31. Cencora did not begin sending out letters to impacted individuals until the week of May 20, 2024. In its letters, Cencora said the data from its systems includes patient names, their postal address and date of birth, as well as information about their health diagnoses and medications.

32. As an entity that collects, creates, and maintains significant volumes of Private Information, the targeted attack was a foreseeable risk of which Cencora was aware and knew it had a duty to guard against.⁸

Cencora Failed to Comply with FTC Guidelines

33. Cencora was prohibited by the Federal Trade Commission Act (the “FTC Act”) (15 U.S.C. § 45) from engaging in “unfair or deceptive acts or practices in or affecting commerce.” The Federal Trade Commission (the “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. *See, e.g., FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015).

34. The FTC has promulgated numerous guides for businesses which 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.

35. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cyber-security guidelines for businesses. The guidelines note that businesses should protect the personal customer information that they keep; properly

⁷ SEC Filing.

⁸ <https://www.cencora.com/global-privacy-statement-overview>. (last visited Feb. 28, 2024) (“Cencora Privacy Policy”).

dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.⁹ The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach. *Id.*

36. The FTC further recommends that companies not maintain Private Information 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.

37. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer 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 Federal Trade Commission Act (“FTCA”), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

38. Cencora failed to properly implement basic data security practices.

39. Cencora’s failure to employ reasonable and appropriate measures to protect against unauthorized access to customers’ Private Information constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

⁹ See ECF No. 1-27, *Protecting Personal Information: A Guide for Business*, Federal Trade Commission (2016).

40. Cencora was at all times fully aware of the obligation to protect the Private Information of Plaintiff and Class Members. Cencora was also aware of the significant repercussions that would result from its failure to do so.

41. Defendants' failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data constitutes an unfair act or practice that violates the FTC Act.

Cencora Failed to Comply with Data Security Industry Standards

42. Experts studying cybersecurity have determined that “[d]ata breaches are both commonplace and costly in the medical industry” and that one of the two sectors within that industry that “sit at the top of the list of the highest average cost of a data breach” is pharmaceuticals.¹⁰

43. Cencora is aware of the importance of safeguarding Plaintiff's and Class Members' Private Information, that by virtue of their business—as a pharmaceutical company—they place Plaintiff's and Class Members' Private Information at risk of being targeted by cybercriminals.

44. Because Cencora failed to implement, maintain, and comply with necessary cybersecurity requirements, as a result, it was unable to protect Plaintiff's and Class Members' information and confidentiality, and protect against obvious and readily foreseeable threats to information security and confidentiality.

45. As a proximate result of such failures, cybercriminals gained unauthorized access to Defendants' networks and acquired Plaintiff's and Class Members' Private Information in the Data Breach without being stopped.

¹⁰ <https://securityintelligence.com/articles/cost-of-a-data-breach-2023-pharmaceutical-industry/> (last visited Mar. 1, 2024).

46. Defendants were unable to prevent the Data Breach and were unable to detect the unauthorized access to vast quantities of sensitive and protected files containing Plaintiff's and Class Members' Private Information.

47. Commonly accepted data security standards among businesses and higher education institutions that store personal information, such as the Private Information involved here, include, but are not limited to:

- a. Maintaining a secure firewall configuration;
- b. Monitoring for suspicious or irregular traffic to servers;
- c. Monitoring for suspicious credentials used to access servers;
- d. Monitoring for suspicious or irregular activity by known users;
- e. Monitoring for suspicious or unknown users;
- f. Monitoring for suspicious or irregular server requests;
- g. Monitoring for server requests for personal and financial information;
- h. Monitoring for server requests from VPNs; and
- i. Monitoring for server requests from Tor exit nodes.

48. The U.S. Federal Trade Commission (“FTC”) publishes guides for businesses for Cybersecurity (Start with Security: A Guide for Business, (June 2015)) and protection of personal and financial information (Protecting Personal Information: A Guide for Business, (Oct. 2016)), which includes basic security standards applicable to all types of businesses and higher education institutions.

49. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer information, 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 Federal Trade Commission Act (“FTC Act”), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses and higher education institutions must take to meet their data security obligations.

50. Because Defendants were entrusted with Plaintiff’s and Class Members’ Private Information, they had and have a duty to keep the Private Information secure.

51. Plaintiff and Class Members reasonably expect that when they entrusted their Private Information to Cencora and Lash Group they will safeguard their information.

52. Despite Defendants’ obligations, Defendants failed to appropriately monitor and maintain their data security systems in a meaningful way so as to prevent the Data Breach.

53. Had Defendants properly maintained their systems and adequately protected them, they could have prevented the Data Breach.

Cencora Violated its Common Law Duty of Reasonable Care

54. Cencora was aware of the importance of security in maintaining personal information (particularly sensitive personal information like the Private Information involved here), and the value consumers place on keeping their Private Information secure.

55. In addition to obligations imposed by federal and state law, Defendants owed and continues to owe a common law duty to Plaintiff and Class Members—who entrusted Defendants with their Private Information—to exercise reasonable care in receiving, maintaining, and storing, the Private Information in Defendant’s possession.

56. Defendants owed and continue to owe a duty to prevent Plaintiff’s and Class Members’ Private Information from being compromised, lost, stolen, accessed, or misused by unauthorized third parties. An essential part of Defendants’ duties were (and are) the obligation to provide reasonable security consistent with current industry best practices and requirements, and

to ensure information technology systems and networks, in addition to the personnel responsible for those systems and networks, adequately protected and continue to protect Plaintiff's and Class Members' PII.

57. Defendants owed a duty to Plaintiff and Class Members, who entrusted Defendants with extremely sensitive Private Information to design, maintain, and test the information technology systems that housed Plaintiff's and Class Members' Private Information, to ensure that the Private Information in Defendants' possession were adequately secured and protected.

58. Defendants owed a duty to Plaintiff and Class Members to create, implement, and maintain reasonable data security practices and procedures sufficient to protect the Private Information stored in Defendants' systems. In addition, this duty also required Cencora and Lash Group to adequately train its employees and others with access to Plaintiff's and Class Members' Private Information on the procedures and practices necessary to safeguard such sensitive information. This duty also required supervision, training, and compliance on Cencora's part to ensure that it complied with creating, implementing, and maintaining reasonable data security practices and procedures sufficient to protect Plaintiff's and Class Members' Private Information.

59. Defendants owed a duty to Plaintiff and Class Members to implement processes that would enable Defendant to timely detect a breach of its information technology systems, and a duty to act upon any data security warnings or red flags detected by such systems in a timely fashion.

60. Defendant owed a duty to Plaintiff and Class Members to disclose when and if their information technology systems and data security practices were not sufficiently adequate to protect and safeguard Plaintiff's and Class Members' Private Information.

61. Thus, Defendants owed a duty to Plaintiff and Class Members to timely disclose

the fact that a data breach, resulting in unauthorized access to their Private Information, had occurred.

62. Defendants violated these duties. The Notice Letter further states that Cencora and Lash Group became aware of the Data Breach on February 21, 2024, however Plaintiff and Class Members, and the public did not learn of the Data Breach until a week later and did not know whether their PII was impacted until Cencora sent out the notice letters in late May 2024. Defendants failed to publicly describe the full extent of the Data Breach and notify affected parties. This demonstrates that Cencora and Lash Group did not properly implement measures designed to timely detect a data breach of their information technology systems, as required to adequately safeguard Plaintiff's and Class Members' Private Information.

63. Defendants also violated their duties to create, implement, and maintain reasonable data security practices and procedures sufficient to protect Plaintiff's and Class Members' Private Information.

64. Cencora and Lash Group breached their obligations to Plaintiff and Class Members and/or were otherwise negligent and reckless because they failed to properly maintain and safeguard their computer systems and data. Cencora's and Lash Group's unlawful conduct includes, but is not limited to, the following acts and/or omissions:

- Failing to maintain an adequate data security system to reduce the risk of data breaches and cyber-attacks;
- Failing to adequately protect customers' Private Information;
- Failing to properly monitor its own data security systems for existing intrusions;
- Failing to ensure that its vendors with access to its computer systems and data employed reasonable security procedures;
- Failing to detect unauthorized ingress into its systems;

- Failing to implement and monitor reasonable network segmentation to detect unauthorized travel within its systems, including to and from areas containing the most sensitive data;
- Failing to detect unauthorized exfiltration of the most sensitive data on its systems;
- Failing to train its employees in the proper handling of emails containing Private Information and maintain adequate email security practices;
- Failing to comply with FTC guidelines for cybersecurity, in violation of Section 5 of the FTC Act;
- Failing to adhere to industry standards for cybersecurity as discussed above; and
- Otherwise breaching its duties and obligations to protect Plaintiff's and Class Members' Private Information.

65. Cencora and Lash Group negligently and unlawfully failed to safeguard Plaintiff's and Class Members Private Information by allowing cybercriminals to access its computer network which contained unsecured and unencrypted Private Information.

66. Had Defendants remedied the deficiencies in their information storage and security systems, followed industry guidelines, and adopted security measures recommended by experts in the field, they could have prevented intrusion into its information storage and security systems and, ultimately, the theft of Plaintiff's and Class Members' confidential Private Information.

67. However, due to Cencora's and Lash Group's failures, Plaintiff and Class Members now face an increased risk of fraud and identity theft. In addition, Plaintiff and the Class Members also lost the benefit of the bargain they made with Cencora and Lash Group.

Cencora Knew or Should Have Known That Criminals Target Private Information and the Data Breach Was Foreseeable and Preventable

68. Defendants were well aware that the protected Private Information it acquires, stores, and utilizes is highly sensitive and of significant value to the owners of the Private Information and those who would use it for wrongful purposes.

69. PII is a valuable commodity to identity thieves, particularly when it is aggregated in large numbers. Former United States Attorney General William P. Barr made clear that consumers' sensitive personal information commonly stolen in data breaches "has economic value." The purpose of stealing large caches of personal data is to use it to defraud individuals or to place it for illegal sale and to profit from other criminals who buy the data and use it to commit fraud and identity theft. Indeed, cybercriminals routinely post stolen personal information on anonymous websites, making the information widely available to the criminal underworld.

70. There is an active and robust market for this information. As John Sancenito, president of Information Network Associates, a company which helps companies with recovery after data breaches, explained after a data breach "[m]ost of the time what [data breach hackers] do is they steal the data and then they sell the data on the dark web to the people who actually commit the fraud."

71. PII is a valuable property right.¹¹ The value of Private Information as a commodity is measurable.¹² "Firms are now able to attain significant market valuations by employing business models predicated on the successful use of personal data within the existing legal and regulatory frameworks."¹³ American companies are estimated to have spent over \$19 billion on acquiring

¹¹ See Marc van Lieshout, *The Value of Personal Data*, 457 IFIP ADVANCES IN INFORMATION AND COMMUNICATION TECHNOLOGY 26 (May 2015), https://www.researchgate.net/publication/283668023_The_Value_of_Personal_Data ("The value of [personal] information is well understood by marketers who try to collect as much data about personal conducts and preferences as possible[.]") (last visited July 6, 2023).

¹² See Robert Lowes, *Stolen EHR [Electronic Health Record] Charts Sell for \$50 Each on Black Market*, MEDSCAPE (Apr. 28, 2014), <http://www.medscape.com/viewarticle/824192> (last visited Mar. 1, 2024).

¹³ *Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value*, OECD 4 (Apr. 2, 2013), https://www.oecd-ilibrary.org/science-and-technology/exploring-the-economics-of-personal-data_5k486qtxldmq-en (last visited Mar. 1, 2024).

personal data of consumers in 2018.¹⁴ Private Information is so valuable to identity thieves that once Private Information has been disclosed, criminals often trade it on the “cyber black-market,” or the “dark web,” for many years.

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

73. The forms of PII involved in this Data Breach are particularly concerning and are a prime target for cybercriminals.

74. The ramifications of Defendants’ failure to keep Plaintiff’s and Class Members’ Private Information secure are long lasting and severe. To avoid detection, identity thieves often hold stolen data for months or years before using it. Also, the sale of stolen information on the “dark web” may take months or more to reach end-users, in part because the data is often sold in small batches as opposed to in bulk to a single buyer. Thus, Plaintiff and Class Members must vigilantly monitor their accounts ad infinitum.

75. Thus, Defendants knew, or should have known, the importance of safeguarding the PII entrusted to it and of the foreseeable consequences if its systems were breached. Defendants failed, however, to take adequate cybersecurity measures to prevent the Data Breach from occurring.

76. As a highly sophisticated party that handles sensitive Private Information,

¹⁴ *U.S. Firms to Spend Nearly \$19.2 Billion on Third-Party Audience Data and Data-Use Solutions in 2018, Up 17.5% from 2017*, INTERACTIVE ADVERTISING BUREAU (Dec. 5, 2018), <https://www.iab.com/news/2018-state-of-data-report/> (last visited Mar. 1, 2024).

Defendants failed to establish and/or implement appropriate administrative, technical and/or physical safeguards to ensure the security and confidentiality of Plaintiff's and other Class Members' Private Information to protect against anticipated threats of intrusion of such information.

77. Moreover, theft of Private Information is also gravely serious because Private Information is an extremely valuable property right.¹⁵

78. Private Information is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the “cyber black-market” for years.

79. There is a strong probability that entire batches of stolen information have been dumped on the black market and are yet to be dumped on the black market, meaning Plaintiff and Class Members are at an increased risk of fraud and identity theft for many years into the future.

80. The Private Information exfiltrated in the Data Breach can also be used to commit identity theft by placing Plaintiff and Class Members at a higher risk of “phishing,” “vishing,” “smishing,” and “pharming,” which are which are other ways for cybercriminals to exploit information they already have in order to get even more personally identifying information from a person through unsolicited email, text messages, and telephone calls purportedly from a legitimate company requesting personal, financial, and/or login credentials.

81. There is often a lag time between when fraud occurs versus when it is discovered, as well as between when Private Information is stolen and when it is used. According to the U.S.

¹⁵ See, e.g., John T. Soma, et al, *Corporate Privacy Trend: The “Value” of Personally Identifiable Information (“PII”) Equals the “Value” of Financial Assets*, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) (“PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.”) (citations omitted) (last accessed Mar. 1, 2024).

Government Accountability Office, which conducted a study regarding data breaches:

[L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.

82. Personal information is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the cyber black market for years. Indeed, a social security number, date of birth, and full name can sell for \$60 to \$80 on the digital black market.¹⁶ “[I]f there is reason to believe that your personal information has been stolen, you should assume that it can end up for sale on the dark web.”¹⁷

83. Plaintiff and Class Members rightfully place a high value not only on their Private Information, but also on the privacy of that data.

84. Thus, Plaintiff and Class Members are at an increased risk of fraud and identity theft for many years into the future. These risks are both certainly impending and substantial. As the FTC has reported, if hackers get access to Private Information, they *will use it*.

85. Data breaches are preventable. As Lucy Thompson wrote in the *Data Breach and Encryption Handbook*, “[i]n almost all cases, the data breaches that occurred could have been prevented by proper planning and the correct design and implementation of appropriate security solutions.” She added that “[o]rganizations that collect, use, store, and share sensitive personal

¹⁶ Michael Kan, *Here’s How Much Your Identity Goes for on the Dark Web*, Nov. 15, 2017, <https://www.pcmag.com/news/heres-how-much-your-identity-goes-for-on-the-dark-web> (last accessed Mar. 1, 2024).

¹⁷ *Dark Web Monitoring: What You Should Know*, Consumer Federation of America, Mar. 19, 2019, https://consumerfed.org/consumer_info/dark-web-monitoring-what-you-should-know/ (last accessed Mar. 1, 2024).

data must accept responsibility for protecting the information and ensuring that it is not compromised...” and “[m]ost of the reported data breaches are a result of lax security and the failure to create or enforce appropriate security policies, rules, and procedures...Appropriate information security controls, including encryption, must be implemented and enforced in a rigorous and disciplined manner so that a data breach never occurs.”

86. This was a financially motivated Data Breach, as the only reason the cybercriminals go through the trouble of running a targeted cyberattack against entities like Cencora is to get information that they can monetize by selling on the black market for use in the kinds of criminal activity described herein. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, “[c]ompared to credit card information, personally identifiable information and Social Security Numbers are worth more than 10x on the black market.”

87. It is within this context that Plaintiff and all other Class Members must now live with the knowledge that their Private Information is forever in cyberspace and was taken by people willing to use the information for any number of improper purposes and scams, including making the information available for sale on the black market.

88. Victims of the Data Breach, like Plaintiff and Class Members, must spend many hours and large amounts of money protecting themselves from the current and future negative impacts to their privacy and credit because of the Data Breach.

89. As a direct and proximate result of the Data Breach, Plaintiff and Class Members have had their PII exposed, have suffered harm as a result, and have been placed at an imminent, immediate, and continuing increased risk of harm from fraud and identity theft. Plaintiff and Class Members must now take the time and effort (and spend the money) to mitigate the actual and

potential impact of the Data Breach on their everyday lives, including purchasing identity theft and credit monitoring services every year for the rest of their lives, placing “freezes” and “alerts” with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, and closely reviewing and monitoring bank accounts, and credit reports for unauthorized activity for years to come.

Defendants Knew or Should Have Known of the Risk Because Healthcare Entities In Possession of Private Information Are Particularly Susceptible to Cyberattacks

90. Defendants’ data security obligations were particularly important given the substantial increase in cyber-attacks and/or data breaches targeting healthcare entities that collect and store Private Information, like Defendants, preceding the date of the breach.

91. Data thieves regularly target companies like Defendants’ due to the highly sensitive information that they custody. Defendants knew and understood that unprotected Private Information is valuable and highly sought after by criminal parties who seek to illegally monetize that Private Information through unauthorized access.

92. In 2021, a record 1,862 data breaches occurred, resulting in approximately 293,927,708 sensitive records being exposed, a 68% increase from 2020.¹⁸

93. Healthcare related breaches, in particular, have continued to rapidly increase because electronic patient data is seen as a valuable asset. In fact, entities that store patient information “have emerged as a primary target because they sit on a gold mine of sensitive personally identifiable information for thousands of patients at any given time. From social security and insurance policies, to next of kin and credit cards, no other organization, including

¹⁸ See 2021 Data Breach Annual Report (ITRC, Jan. 2022) (available at <https://notified.idtheftcenter.org/s/>), at 6.

credit bureaus, have so much monetizable information stored in their data centers.”¹⁹

94. Moreover, in light of recent high profile data breaches at other industry leading companies, including, Microsoft (250 million records, December 2019), Wattpad (268 million records, June 2020), Facebook (267 million users, April 2020), Estee Lauder (440 million records, January 2020), Whisper (900 million records, March 2020), and Advanced Info Service (8.3 billion records, May 2020), Defendants knew or should have known that the Private Information that they collected and maintained would be targeted by cybercriminals.

95. As a custodian of Private Information, Defendants knew, or should have known, the importance of safeguarding the Private Information entrusted to it by Plaintiff and Class Members, and of the foreseeable consequences if their data security systems were breached, including the significant costs imposed on Plaintiff and Class Members as a result of a breach.

96. Despite the prevalence of public announcements of data breach and data security compromises, Defendants failed to take appropriate steps to protect the Private Information of Plaintiff and Class Members from being compromised.

97. At all relevant times, Defendants knew, or reasonably should have known, of the importance of safeguarding the Private Information of Plaintiff and Class Members and of the foreseeable consequences that would occur if Defendants' data security system was breached, including, specifically, the significant costs that would be imposed on Plaintiffs and Class Members as a result of a breach.

98. Additionally, as companies became more dependent on computer systems to run

¹⁹ Inside Digital Health, *How to Safeguard Hospital Data from Email Spoofing Attacks*, April 4, 2019, available at: <https://www.chiefhealthcareexecutive.com/view/how-to-safeguard-hospital-data-from-email-spoofing-attacks> (last visited on Sept. 13, 2023).

their business,²⁰ *e.g.*, working remotely as a result of the Covid-19 pandemic, and the Internet of Things (“IoT”), the danger posed by cybercriminals is magnified, thereby highlighting the need for adequate administrative, physical, and technical safeguards.²¹

99. Defendants were, or should have been, fully aware of the unique type and the significant volume of data on Defendants’ servers, amounting to potentially hundreds of thousands individuals’ detailed Private Information, and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

100. The injuries to Plaintiff and Class Members were directly and proximately caused by Defendants’ failure to implement or maintain adequate data security measures for the Private Information of Plaintiff and Class Members.

101. The ramifications of Defendants’ failure to keep secure the Private Information of Plaintiff and Class Members are long lasting and severe. Once Private Information is stolen—particularly PHI—fraudulent use of that information and damage to victims may continue for years.

102. As a healthcare services company in possession of current and former patients’ Private Information, Defendants knew, or should have known, the importance of safeguarding the Private Information entrusted to them by Plaintiff and Class Members and of the foreseeable consequences if their data security systems were breached. This includes the significant costs imposed on Plaintiff and Class Members as a result of a breach. Nevertheless, Defendants failed to take adequate cybersecurity measures to prevent the Data Breach.

²⁰ <https://www.federalreserve.gov/econres/notes/feds-notes/implications-of-cyber-risk-for-financial-stability-20220512.html> (last accessed Sept. 13, 2023).

²¹ <https://www.picussecurity.com/key-threats-and-cyber-risks-facing-financial-services-and-banking-firms-in-2022> (last accessed Sept. 13, 2023).

Plaintiff and Class Members Suffered Harm as a Result of the Data Breach

103. The ramifications of Defendants' failure to keep Private Information secure are long-lasting and severe. Victims of data breaches are more likely to become victims of identity fraud, occurring 65 percent of the time. In 2019 alone, consumers lost more than \$1.9 billion to identity theft and fraud.

104. Besides damage sustained in the event of identity theft, consumers may also spend anywhere from approximately 7 hours to upwards to over 1,000 hours trying to resolve identity theft issues. The Department of Justice's Bureau of Justice Statistics found that "among victims who had personal information used for fraudulent purposes, 29% spent a month or more resolving problems."

105. Plaintiff's and Class Members' Private Information was provided to Cencora in conjunction with the type of work Cencora performs as a pharmaceutical provider. In requesting and maintaining Plaintiff's and Class Members' Private Information, Cencora promised, and undertook a duty, to act reasonably in its handling of Plaintiff's and Class Members' Private Information. Cencora, however, did not take proper care of Plaintiff's and Class Members' Private Information, leading to its exposure to and exfiltration by cybercriminals as a direct result of Cencora's inadequate data security measures.

106. As a result of Cencora's conduct and failure to implement adequate and reasonable cybersecurity procedures and protocols necessary to protect consumers' Private Information, which allowed the Data Breach to occur, Plaintiff's and Class Members' Private Information has been and is now in the hands of unauthorized individuals and third parties, which may include thieves, unknown criminals, banks, credit companies, and other potentially hostile individuals.

107. Plaintiff and Class Members greatly value their privacy, especially their highly-

sensitive information, such as their first and last names, dates of birth, addresses, and medical information. They would not have entrusted Cencora with this highly-sensitive information, had they known that Cencora would negligently fail to adequately protect their Private Information. Indeed, Plaintiff and Class Members provided Cencora with this highly-sensitive information with the expectation that Cencora would keep their Private Information secure and inaccessible from unauthorized parties.

108. As a result of Cencora's failure to implement and follow even the most basic security procedures, Plaintiff and Class Members suffered actual damages including, without limitation, time and expenses related to monitoring their financial accounts for fraudulent activity, exposure to increased and imminent risk of fraud and identity theft, the loss in value of their personal information, and other economic and non-economic harm. Plaintiff and Class Members will now be forced to expend additional time to review their credit reports and monitor their financial accounts and medical records for fraud or identify theft—particularly since the compromised information may include Social Security numbers.

109. Once Private Information is exposed, there is virtually no way to ensure that the exposed information has been fully recovered or contained against future misuse. For this reason, Plaintiff and Class Members will need to maintain these heightened measures for years, and possibly their entire lives.

110. Plaintiff and Class Members are also at a continued risk of harm because their Private Information remains in Cencora's systems, which have already been shown to be susceptible to compromise and attack and is subject to further attack so long as Cencora fails to undertake the necessary and appropriate data security measures to protect the Private Information in its possession.

111. As a result of the Data Breach, and in addition to the time Plaintiff and Class Members have spent and anticipate spending to mitigate the impact of the Data Breach on their lives, Plaintiff and Class Members have also suffered emotional distress from the public release of their Private Information, which they believed would be protected from unauthorized access and disclosure. The emotional distress they have experienced includes anxiety and stress resulting from the fear that unauthorized bad actors are viewing, selling, and or using their Private Information for the purposes of identity theft and fraud.

112. Additionally, Plaintiff and Class Members have suffered damage to and diminution in the value of their highly sensitive and confidential Private Information —a form of property that Plaintiff and Class Members entrusted to Cencora and which was compromised as a result of the Data Breach Cencora failed to prevent. Plaintiff and Class Members have also suffered a violation of their privacy rights as a result of Cencora’s unauthorized disclosure of their Private Information.

CLASS ACTION ALLEGATIONS

113. Plaintiff brings this case individually and, pursuant to Rule 23(b)(2), (b)(3), and (c)(4) of the Federal Rules of Civil Procedure, on behalf of the following Nationwide Class and state classes (collectively the “Class”):

Nationwide Class

All persons whose Private Information was compromised in the Data Breach that was discovered by Cencora on or around February 21, 2021.

In addition, or in the alternative, Plaintiff proposes the following state class:

Ohio Class

All residents of Ohio whose Private Information was compromised in the Data breach that was discovered by Cencora on or around February 21, 2021.

114. Excluded from the Class is Cencora, its subsidiaries and affiliates, its officers,

directors and members of their immediate families and any entity in which Cencora has 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.

115. Plaintiff reserves the right to modify or amend the definition of the proposed Class, if necessary, before this Court determines whether certification is appropriate.

116. The requirements of Rule 23(a)(1) are satisfied. The Class described above is so numerous that joinder of all individual members in one action would be impracticable. The disposition of the individual claims of the respective Class Members through this class action will benefit both the parties and this Court. As noted above, there are approximately 500,000 Class Members.

117. The exact size of the Class and the identities of the individual members thereof are ascertainable through Defendants' records, including but not limited to, the information implicated in the Data Breach.

118. The requirements of Rule 23(a)(2) are satisfied. There is a well-defined community of interest and there are common questions of fact and law affecting Class Members. The questions of fact and law common to the Class predominate over questions which may affect individual members and include the following:

- a. Whether and to what extent Defendants had a duty to secure and protect the Private Information of Plaintiff and Class Members;
- b. Whether Defendants were negligent in collecting and disclosing Plaintiff's and Class Members' Private Information;

- c. Whether Defendants had duties not to disclose the PII of Plaintiff and Class Members to unauthorized third parties;
- d. Whether Defendants took reasonable steps and measures to safeguard Plaintiff's and Class Members' Private Information;
- e. Whether Defendants failed to adequately safeguard the Private Information of Plaintiff and Class Members;
- f. Whether Defendants breached their duties to exercise reasonable care in handling Plaintiff's and Class Members' Private Information in the manner alleged herein, including failing to comply with industry standards;
- g. Whether Defendants failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;
- h. Whether Defendants had respective duties not to use the Private Information of Plaintiff and Class Members for non-business purposes;
- i. Whether Defendants adequately, promptly, and accurately informed Plaintiff and Class Members that their Private Information had been compromised;
- j. Whether Plaintiff and Class Members are entitled to declaratory judgment under 28 U.S.C. § 2201, *et seq.*;
- k. Whether Plaintiff and Class Members are entitled to damages as a result of Defendants' wrongful conducts; and

1. Whether Plaintiff and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach.

119. The requirements of Rule 23(a)(3) are satisfied. Plaintiff's claims are typical of the claims of Class Members. The claims of the Plaintiff and Class Members are based on the same legal theories and arise from the same failure by Defendants to safeguard Private Information. Plaintiff and Class Members each had their Private Information disclosed by Defendants to an unauthorized third party.

120. The requirements of Rule 23(a)(4) are satisfied. Plaintiff is an adequate representative of the Class because his interests do not conflict with the interests of the Class Members. Plaintiff will fairly, adequately, and vigorously represent and protect the interests of Class Members and have 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, including data breach litigation. The claims of Plaintiff and Class Members are substantially identical as explained above. While the aggregate damages that may be awarded to the Class Members are likely to be substantial, the damages suffered by the individual Class Members are relatively small. As a result, the expense and burden of individual litigation make it economically infeasible and procedurally impracticable for each member of the Class to individually seek redress for the wrongs done to them. Certifying the case as a class will centralize these substantially identical claims in a single proceeding, which is the most manageable litigation method available to Plaintiff and the Class and will conserve the resources of the parties and the court system, while protecting the rights of each member of the Class. Defendants' uniform conduct is generally applicable to the Class as a whole, making relief appropriate with respect to each Class Member.

121. Here a class action is superior to other available methods for the fair and efficient adjudication of this controversy. The adjudication of this controversy through a class action will avoid the possibility of inconsistent and potentially conflicting adjudications of the asserted claims. There will be no difficulty in managing this action as a class action, and the disposition of the claims of the Class members in a single action will provide substantial benefits to all parties and to the Court. Damages for any individual Class Member are likely insufficient to justify the cost of individual litigation so that, in the absence of class treatment, Defendants' violations of law inflicting damages in the aggregate would go un-remedied.

122. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

- a. Whether Defendants owed a legal duty to Plaintiff and the Classes to exercise due care in collecting, storing, using, and safeguarding their Private Information;
- b. Whether Defendants' data security practices were reasonable in light of best practices recommended by data security experts;
- c. Whether Defendants' failure to institute adequate protective security measures amounted to negligence;
- d. Whether Defendants failed to take commercially reasonable steps to safeguard consumer Private Information; and

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

123. Finally, all members of the proposed Classes are readily ascertainable. Defendants have access to Class Members' names and addresses affected by the Data Breach. At least some Class Members have already been preliminarily identified and sent notice of the Data Breach by Defendants.

CAUSES OF ACTION

COUNT I **NEGLIGENCE**

(On Behalf of Plaintiff and the Nationwide Class or, Alternatively, the Pennsylvania Class)

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

125. Cencora and Lash Group owed a duty to Plaintiff and all other Class Members to exercise reasonable care in safeguarding and protecting their Private Information in its possession, custody, or control.

126. Cencora and Lash Group knew, or should have known, the risks of collecting and storing Plaintiff's and all other Class Members' Private Information and the importance of maintaining secure systems. Cencora and Lash Group knew, or should have known, of the vast uptick in data breaches in recent years. Cencora and Lash Group had a duty to protect the Private Information of Plaintiff and Class Members.

127. Given the nature of Cencora's and Lash Group's businesses, the sensitivity and value of the Private Information it maintains, and the resources at its disposal, Cencora and Lash Group should have identified the vulnerabilities to its systems and prevented the Data Breach from

occurring, which Cencora and Lash Group had a duty to prevent.

128. Cencora and Lash Group breached these duties by failing to exercise reasonable care in safeguarding and protecting Plaintiff's and Class Members' Private Information by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems to safeguard and protect Private Information entrusted to them—including Plaintiff's and Class Members' Private Information.

129. It was reasonably foreseeable to Cencora and Lash Group that their failure to exercise reasonable care in safeguarding and protecting Plaintiff's and Class Members' Private Information by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems would result in the unauthorized release, disclosure, and dissemination of Plaintiff's and Class Members' Private Information to unauthorized individuals.

130. But for Cencora's and Lash Group's negligent conduct/breach of the above-described duties owed to Plaintiff and Class Members, their PII would not have been compromised.

131. As a result of Cencora's and Lash Group's above-described wrongful actions, inaction, and want of ordinary care that directly and proximately caused the Data Breach, Plaintiff and all other Class Members have suffered, and will continue to suffer, economic damages and other injury and actual harm in the form of, *inter alia*: (i) a substantially increased risk of identity theft and medical theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (ii) improper disclosure of their Private Information; (iii) breach of the confidentiality of their Private Information; (iv) deprivation of the value of their

Private Information, for which there is a well-established national and international market; (v) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of medical identity theft they face and will continue to face; and (vii) actual or attempted fraud.

COUNT II
NEGLIGENCE *PER SE*

(On Behalf of Plaintiff and the Nationwide Class, or Alternatively, the Pennsylvania Class)

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

133. In addition to the common law, Cencora's and Lash Group's duties arise from Section 5 of the FTCA ("FTCA"), 15 U.S.C. § 45(a)(1), which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted by the FTC, the unfair act or practice by a business, such as Cencora and Lash Group, of failing to employ reasonable measures to protect and secure Private Information.

134. Cencora and Lash Group violated Section 5 of the FTCA by failing to use reasonable measures to protect Plaintiff's and all other Class Members' Private Information and not complying with applicable industry standards. Cencora's and Lash Group's conduct were particularly unreasonable given the nature and amount of Private Information it obtains and stores, and the foreseeable consequences of a data breach involving Private Information including, specifically, the substantial damages that would result to Plaintiff and the other Class Members.

135. Cencora's and Lash Group's violations of Section 5 of the FTCA constitutes negligence *per se*.

136. Plaintiff and Class Members are within the class of persons that Section 5 of the FTCA was intended to protect.

137. The harm occurring as a result of the Data Breach is the type of harm Section 5 of the FTCA was intended to guard against.

138. It was reasonably foreseeable to Cencora and Lash Group that their failure to exercise reasonable care in safeguarding and protecting Plaintiff's and Class Members' Private Information by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems, would result in the release, disclosure, and dissemination of Plaintiff's and Class Members' Private Information to unauthorized individuals.

139. The injury and harm that Plaintiff and the other Class Members suffered was the direct and proximate result of Cencora's and Lash Group's violations of Section 5 of the FTCA. Plaintiff and Class Members have suffered (and will continue to suffer) economic damages and other injury and actual harm in the form of, *inter alia*: (i) a substantially increased risk of identity theft and medical theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (ii) improper disclosure of their Private Information; (iii) breach of the confidentiality of their Private Information; (iv) deprivation of the value of their Private Information, for which there is a well-established national and international market; (v) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of medical identity theft they face and will continue to face; and (vi) actual or attempted fraud.

COUNT III
BREACH OF FIDUCIARY DUTY
(On Behalf of Plaintiff and the Nationwide Class or, Alternatively, the Pennsylvania Class)

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

141. Plaintiff and Class Members either directly or indirectly gave Cencora and Lash Group their Private Information in confidence, believing that Cencora and Lash Group – healthcare organizations – would protect that information. Plaintiff and Class Members would not have provided Cencora and Lash Group with this information had they known it would not be adequately protected. Cencora's and Lash Group's acceptance and storage of Plaintiff's and Class Members' Private Information created a fiduciary relationship between Defendants and Plaintiff and Class Members. In light of this relationship, Cencora and Lash Group must act primarily for the benefit of its patients (at least insofar as it relates to the safeguarding of their PII).

142. Cencora has a fiduciary duty to act for the benefit of Plaintiff and Class Members upon matters within the scope of their relationship. It breached that duty by failing to properly protect the integrity of the system containing Plaintiff's and Class Members' Private Information, failing to comply with the data security guidelines set forth by Section 5 of the FTCA, and otherwise failing to safeguard the Private Information of Plaintiff and Class Members it collected.

143. As a direct and proximate result of Cencora's and Lash Group's breaches of its fiduciary duties, Plaintiff and Class Members have suffered and will suffer injury, including, but not limited to: (i) a substantial increase in the likelihood of identity theft; (ii) the compromise, publication, and theft of their Private Information; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from unauthorized use of their Private Information; (iv) lost opportunity costs associated with effort attempting to mitigate the actual and future consequences of the Data Breach; (v) the continued risk to their Private Information which remains in Cencora's and Lash Group's possession; (vi) future costs in terms of time, effort, and money that will be required to prevent, detect, and repair the impact of the Private Information compromised as a result of the Data Breach; and (vii) actual or attempted fraud.

COUNT IV
UNJUST ENRICHMENT
(On Behalf of Plaintiff and the Nationwide Class or, Alternatively, the Pennsylvania Class)

144. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein. This claim is pled in the alternative to the implied contract claim pursuant to Fed. R. Civ. P. 8(d)(2).

145. Plaintiff and Class Members conferred a monetary benefit upon Cencora and Lash Group in the form of monies paid for educational services or other services.

146. Cencora and Lash Group accepted or had knowledge of the benefits conferred upon them by Plaintiff and Class Members. Cencora and Lash Group also benefited from the receipt of Plaintiff's and Class Members' Private Information.

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

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

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

COUNT V
BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiff and the Nationwide Class or, Alternatively, the Pennsylvania Class)

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

151. Defendants required Plaintiff and Class Members to provide, or authorize the transfer of, their Private Information in order for Cencora and Lash Group to healthcare and patient services. In exchange, Cencora and Lash Group entered into implied contracts with Plaintiff and Class Members in which Cencora and Lash Group agreed to comply with their statutory and common law duties to protect Plaintiff's and Class Members' Private Information and to timely notify them in the event of a data breach.

152. Plaintiff and Class Members would not have provided their Private Information to Defendants had they known that Defendants would not safeguard their Private Information, as promised, or provide timely notice of a data breach.

153. Plaintiff and Class Members fully performed their obligations under their implied contracts with Defendants.

154. Defendants breached the implied contracts by failing to safeguard Plaintiff's and Class Members' Private Information and by failing to provide them with timely and accurate notice of the Data Breach.

155. The losses and damages Plaintiff and Class Members sustained (as described above) were the direct and proximate result of Defendants' breach of their implied contracts with Plaintiff and Class Members.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff on behalf of himself and all others similarly situated, prays for

relief as follows:

- (a) 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;
- (b) For an order finding in favor of Plaintiff and the Class on all counts asserted herein;
- (c) For damages, including all compensatory, punitive, and/or nominal damages, in an amount to be determined by the trier of fact;
- (d) For an order of restitution and all other forms of equitable monetary relief;
- (e) Declaratory and injunctive relief as described herein;
- (f) Awarding Plaintiff and the Class reasonable attorneys' fees, costs, and expenses;
- (g) Awarding pre- and post-judgment interest on any amounts awarded; and
- (h) Awarding such other and further relief as may be just and proper.

JURY TRIAL DEMAND

A jury trial is demanded on all claims so triable.

Date: May 24, 2024

Respectfully Submitted,


/s/ 

Jonathan Shub (PA Bar 53965)
Benjamin F. Johns (PA Bar 201373)
Samantha E. Holbrook (PA Bar 311829)
Andrea L. Bonner (PA Bar 332945)
SHUB & JOHNS LLC
Four Tower Bridge
200 Barr Harbor Drive, Suite 400
Conshohocken, PA 19428
Telephone: (610) 477-8380
Fax: (856) 210-9088
jshub@shublawyers.com
bjohns@shublawyers.com
sholbrook@shublawyers.com
abonner@shublawyers.com

Gary M. Klinger*
Mariya Weekes*
MILBERG COLEMAN BRYSON
PHILLIPS GROSSMAN LLC
227 W. Monroe Street, Suite 2100
Chicago, IL 60606
Phone: (866) 252-0878
gklinger@milberg.com
mweekes@milberg.com

Co-Lead Counsel for Plaintiffs

**pro hac vice forthcoming*

CERTIFICATE OF SERVICE

I HEREBY CERTIFY that on this 24th day of May 2024, I electronically filed the foregoing with the Clerk of the Court using the CM/ECF system which will send notification of such filing to the e-mail addresses denoted on the Electronic Mail notice list.

/s/ Benjamin F. Johns

Benjamin F. Johns