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

MAURISA CASTELLANO, individually and on behalf of all others similarly situated, Plaintiff, v. CENCORA, INC. and THE LASH GROUP, LLC, Defendants.	Case No. 24-2568 **CLASS ACTION** **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Plaintiff Maurisa Castellano ("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 her 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. In late May 2024, following Defendant Cencora's SEC Filing, several of its pharmaceutical company clients began notifying state Attorneys General about the impact of the data breach. It has been reported that at least 23 pharmaceutical and biotechnology companies were impacted by the breach. These companies include Abbot, AbbVie Inc., Acadia Pharmaceuticals Inc., Amgen Inc., Bausch Health Companies Inc., Bayer Corporation, Bristol Myers Squibb Company and Bristol Myers Squibb Patient Assistance Foundation, Dendreon Pharmaceuticals LLC, Endo Pharmaceuticals Inc., Genentech, Inc., GlaxoSmithKline Group of

[2] https://investor.amerisourcebergen.com/financials/sec-filings/default.aspx (last visited Feb. 29, 2024) ("SEC Filing").
[3] *Id.*

Companies and the GlaxoSmithKline Patient Access Programs Foundation, Heron Therapeutics, Inc., Incyte Corporation, Johnson & Johnson Services, Inc. and Johnson & Johnson Patient Assistance Foundation, Inc., Marathon Pharmaceuticals, LLC/PTC Therapeutics, Inc., Novartis Pharmaceuticals Corporation, Otsuka American Pharmaceutical, Inc., Pharming Healthcare, Inc., Rayner Surgical Inc., Regeneron Pharmaceuticals, Inc., Sandoz Inc., Sumitomo Pharma America, Inc. / Sunovion Pharmaceuticals Inc., Takeda Pharmaceuticals U.S.A., Inc., and Tolmar.[4]

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

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

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

8. Plaintiff brings this class action lawsuit on behalf of those similarly situated to 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 Maurisa Castellano

9. Plaintiff Maurisa Castellano at all relevant times was and is a resident and citizen of Houston, Texas.

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

11. On or around May 28, 2024, Defendants notified Plaintiff Castellano that the

[4] *See* www.hipaajournal.com/cencora-cyberattack-data-breach/ (last visited June 11, 2024).

Defendants' network had been accessed and Plaintiff's Private Information may have been involved in the Data Breach.

12. As a result of the Data Breach, Plaintiff Castellano spent considerable time dealing with the consequences of the Data Breach, and will now need to dedicate additional time to self-monitor her accounts and credit reports to ensure no fraudulent activity has occurred.

13. Plaintiff also suffered real damages as a result of the Data Breach within Defendants' systems. In or around February 2024, Plaintiff was contacted by a vehicle dealership indicating that there was an attempt to purchase a vehicle using Plaintiff Castellano's information, for which Plaintiff replied that that transaction was fraudulent. Similarly, in or around March 2024, Plaintiff received a payment card from a financial institution, whom she subsequently contacted to discover that a bank account had been opened using her personal information. Plaintiff expressed to the financial institution that the bank account was opened fraudulently.

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

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

B. <u>Defendant Cencora, Inc.</u>

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.[5] Cencora is a pharmaceutical services company that provides distribution solutions for doctor's offices,

[5] *Id.*

pharmacies, and animal healthcare.[6]

C. Defendant Cencora, Inc.

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.[7]

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 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 Castellano 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.

---

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

[7] https://www.lashgroup.com/ (last visited May 24, 2024)

21. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(a)(1) because a substantial part of the events giving rise to this action occurred in this District. 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."[8]

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.

[8] SEC Filing.

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.[9]

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 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.[10] 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

[9] https://www.cencora.com/global-privacy-statement-overview. (last visited Feb. 28, 2024) ("Cencora Privacy Policy").

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

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.

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.[11]

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.

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:

---

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

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 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.[12] The value of Private Information as a commodity is measurable.[13] "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."[14] American companies are estimated to have spent over $19 billion on acquiring personal data of consumers in 2018.[15] 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

---

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

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

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

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

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, 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.[16]

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. 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.

[16] *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).

> 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.[17] "[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."[18]

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 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

---

[17] 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).

[18] *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).

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 Suspectable 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.[19]

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 credit bureaus, have so much monetizable information stored in their data centers."[20]

---

[19] *See* 2021 Data Breach Annual Report (ITRC, Jan. 2022) (available at https://notified.idtheftcenter.org/s/), at 6.

[20] 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).

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 their business,[21] *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

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

for adequate administrative, physical, and technical safeguards.[22]

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.

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

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

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:

> **Texas Class**

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

l. 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 her 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 Texas 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 Texas 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 Texas 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 Texas 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 Texas 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 herself 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.

Dated: June 11, 2024

Benjamin F. Johns (PA Bar No. 201373)
Samantha E. Holbrook (PA Bar No. 311829)
Andrea L. Bonner (PA Bar 332945)
SHUB & JOHNS LLC
Four Tower Bridge
200 Barr Harbor Drive, Suite 400
Conshohocken, PA 19428
Phone: (610) 477-8380
bjohns@shublawyers.com
sholbrook@shublawyers.com
abonner@shublawyers.com

Terence R. Coates*
Jonathan T. Deters*
MARKOVITS, STOCK & DeMARCO, LLC
119 E. Court Street, Suite 530
Cincinnati, Ohio 45202
Telephone: (513) 651-3700
Facsimile: (513) 665-0219
tcoates@msdlegal.com
jdeters@msdlegal.com

**pro hac vice forthcoming*

Attorneys for Plaintiffs and the putative class

JS 44 (Rev. 04/21)

CIVIL COVER SHEET

The JS 44 civil cover sheet and the information contained herein neither replace nor supplement the filing and service of pleadings or other papers as required by law, except as provided by local rules of court. This form, approved by the Judicial Conference of the United States in September 1974, is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. *(SEE INSTRUCTIONS ON NEXT PAGE OF THIS FORM.)*

I. (a) PLAINTIFFS

Maurisa Castellano

(b) County of Residence of First Listed Plaintiff Harris County
(EXCEPT IN U.S. PLAINTIFF CASES)

(c) Attorneys *(Firm Name, Address, and Telephone Number)*
Benjamin F. Johns, Esq., Shub & Johns LLC, Four Tower Bridge, 200 Barr Harbor Drive, Suite 400, Conshohocken, PA 19428 Tel.: 610.477.8380, bjohns@shublawyers.com

DEFENDANTS

Cencora, Inc.

County of Residence of First Listed Defendant Montgomery
(IN U.S. PLAINTIFF CASES ONLY)

NOTE: IN LAND CONDEMNATION CASES, USE THE LOCATION OF THE TRACT OF LAND INVOLVED.

Attorneys *(If Known)*

II. BASIS OF JURISDICTION *(Place an "X" in One Box Only)*

- ☐ 1 U.S. Government Plaintiff
- ☐ 3 Federal Question *(U.S. Government Not a Party)*
- ☐ 2 U.S. Government Defendant
- ☒ 4 Diversity *(Indicate Citizenship of Parties in Item III)*

III. CITIZENSHIP OF PRINCIPAL PARTIES *(Place an "X" in One Box for Plaintiff and One Box for Defendant)*

(For Diversity Cases Only)

	PTF	DEF		PTF	DEF
Citizen of This State	☐ 1	☐ 1	Incorporated *or* Principal Place of Business In This State	☐ 4	☒ 4
Citizen of Another State	☒ 2	☐ 2	Incorporated *and* Principal Place of Business In Another State	☐ 5	☐ 5
Citizen or Subject of a Foreign Country	☐ 3	☐ 3	Foreign Nation	☐ 6	☐ 6

IV. NATURE OF SUIT *(Place an "X" in One Box Only)*

Click here for: Nature of Suit Code Descriptions.

CONTRACT
- ☐ 110 Insurance
- ☐ 120 Marine
- ☐ 130 Miller Act
- ☐ 140 Negotiable Instrument
- ☐ 150 Recovery of Overpayment & Enforcement of Judgment
- ☐ 151 Medicare Act
- ☐ 152 Recovery of Defaulted Student Loans (Excludes Veterans)
- ☐ 153 Recovery of Overpayment of Veteran's Benefits
- ☐ 160 Stockholders' Suits
- ☐ 190 Other Contract
- ☐ 195 Contract Product Liability
- ☐ 196 Franchise

TORTS

PERSONAL INJURY
- ☐ 310 Airplane
- ☐ 315 Airplane Product Liability
- ☐ 320 Assault, Libel & Slander
- ☐ 330 Federal Employers' Liability
- ☐ 340 Marine
- ☐ 345 Marine Product Liability
- ☐ 350 Motor Vehicle
- ☐ 355 Motor Vehicle Product Liability
- ☒ 360 Other Personal Injury
- ☐ 362 Personal Injury - Medical Malpractice

PERSONAL INJURY
- ☐ 365 Personal Injury - Product Liability
- ☐ 367 Health Care/ Pharmaceutical Personal Injury Product Liability
- ☐ 368 Asbestos Personal Injury Product Liability

PERSONAL PROPERTY
- ☐ 370 Other Fraud
- ☐ 371 Truth in Lending
- ☐ 380 Other Personal Property Damage
- ☐ 385 Property Damage Product Liability

FORFEITURE/PENALTY
- ☐ 625 Drug Related Seizure of Property 21 USC 881
- ☐ 690 Other

LABOR
- ☐ 710 Fair Labor Standards Act
- ☐ 720 Labor/Management Relations
- ☐ 740 Railway Labor Act
- ☐ 751 Family and Medical Leave Act
- ☐ 790 Other Labor Litigation
- ☐ 791 Employee Retirement Income Security Act

IMMIGRATION
- ☐ 462 Naturalization Application
- ☐ 465 Other Immigration Actions

BANKRUPTCY
- ☐ 422 Appeal 28 USC 158
- ☐ 423 Withdrawal 28 USC 157

INTELLECTUAL PROPERTY RIGHTS
- ☐ 820 Copyrights
- ☐ 830 Patent
- ☐ 835 Patent - Abbreviated New Drug Application
- ☐ 840 Trademark
- ☐ 880 Defend Trade Secrets Act of 2016

SOCIAL SECURITY
- ☐ 861 HIA (1395ff)
- ☐ 862 Black Lung (923)
- ☐ 863 DIWC/DIWW (405(g))
- ☐ 864 SSID Title XVI
- ☐ 865 RSI (405(g))

FEDERAL TAX SUITS
- ☐ 870 Taxes (U.S. Plaintiff or Defendant)
- ☐ 871 IRS—Third Party 26 USC 7609

OTHER STATUTES
- ☐ 375 False Claims Act
- ☐ 376 Qui Tam (31 USC 3729(a))
- ☐ 400 State Reapportionment
- ☐ 410 Antitrust
- ☐ 430 Banks and Banking
- ☐ 450 Commerce
- ☐ 460 Deportation
- ☐ 470 Racketeer Influenced and Corrupt Organizations
- ☐ 480 Consumer Credit (15 USC 1681 or 1692)
- ☐ 485 Telephone Consumer Protection Act
- ☐ 490 Cable/Sat TV
- ☐ 850 Securities/Commodities/ Exchange
- ☐ 890 Other Statutory Actions
- ☐ 891 Agricultural Acts
- ☐ 893 Environmental Matters
- ☐ 895 Freedom of Information Act
- ☐ 896 Arbitration
- ☐ 899 Administrative Procedure Act/Review or Appeal of Agency Decision
- ☐ 950 Constitutionality of State Statutes

REAL PROPERTY
- ☐ 210 Land Condemnation
- ☐ 220 Foreclosure
- ☐ 230 Rent Lease & Ejectment
- ☐ 240 Torts to Land
- ☐ 245 Tort Product Liability
- ☐ 290 All Other Real Property

CIVIL RIGHTS
- ☐ 440 Other Civil Rights
- ☐ 441 Voting
- ☐ 442 Employment
- ☐ 443 Housing/ Accommodations
- ☐ 445 Amer. w/Disabilities - Employment
- ☐ 446 Amer. w/Disabilities - Other
- ☐ 448 Education

PRISONER PETITIONS

Habeas Corpus:
- ☐ 463 Alien Detainee
- ☐ 510 Motions to Vacate Sentence
- ☐ 530 General
- ☐ 535 Death Penalty

Other:
- ☐ 540 Mandamus & Other
- ☐ 550 Civil Rights
- ☐ 555 Prison Condition
- ☐ 560 Civil Detainee - Conditions of Confinement

V. ORIGIN *(Place an "X" in One Box Only)*

☒ 1 Original Proceeding ☐ 2 Removed from State Court ☐ 3 Remanded from Appellate Court ☐ 4 Reinstated or Reopened ☐ 5 Transferred from Another District *(specify)* ☐ 6 Multidistrict Litigation - Transfer ☐ 8 Multidistrict Litigation - Direct File

VI. CAUSE OF ACTION

Cite the U.S. Civil Statute under which you are filing ***(Do not cite jurisdictional statutes unless diversity)***:
28 U.S.C 1332(d)

Brief description of cause:
Data Breach class action.

VII. REQUESTED IN COMPLAINT:

☒ CHECK IF THIS IS A **CLASS ACTION** UNDER RULE 23, F.R.Cv.P.

DEMAND $ $5,000,000

CHECK YES only if demanded in complaint:
JURY DEMAND: ☒ Yes ☐ No

VIII. RELATED CASE(S) IF ANY

(See instructions): JUDGE Cynthia M. Rufe DOCKET NUMBER 2:2024-cv-02227

DATE 6.12.2024

SIGNATURE OF ATTORNEY OF RECORD s/ Benjamin F. Johns

FOR OFFICE USE ONLY

RECEIPT # _____ AMOUNT _____ APPLYING IFP _____ JUDGE _____ MAG. JUDGE _____

INSTRUCTIONS FOR ATTORNEYS COMPLETING CIVIL COVER SHEET FORM JS 44

Authority For Civil Cover Sheet

The JS 44 civil cover sheet and the information contained herein neither replaces nor supplements the filings and service of pleading or other papers as required by law, except as provided by local rules of court. This form, approved by the Judicial Conference of the United States in September 1974, is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. Consequently, a civil cover sheet is submitted to the Clerk of Court for each civil complaint filed. The attorney filing a case should complete the form as follows:

I.(a) **Plaintiffs-Defendants.** Enter names (last, first, middle initial) of plaintiff and defendant. If the plaintiff or defendant is a government agency, use only the full name or standard abbreviations. If the plaintiff or defendant is an official within a government agency, identify first the agency and then the official, giving both name and title.

(b) **County of Residence.** For each civil case filed, except U.S. plaintiff cases, enter the name of the county where the first listed plaintiff resides at the time of filing. In U.S. plaintiff cases, enter the name of the county in which the first listed defendant resides at the time of filing. (NOTE: In land condemnation cases, the county of residence of the "defendant" is the location of the tract of land involved.)

(c) **Attorneys.** Enter the firm name, address, telephone number, and attorney of record. If there are several attorneys, list them on an attachment, noting in this section "(see attachment)".

II. **Jurisdiction.** The basis of jurisdiction is set forth under Rule 8(a), F.R.Cv.P., which requires that jurisdictions be shown in pleadings. Place an "X" in one of the boxes. If there is more than one basis of jurisdiction, precedence is given in the order shown below.
United States plaintiff. (1) Jurisdiction based on 28 U.S.C. 1345 and 1348. Suits by agencies and officers of the United States are included here.
United States defendant. (2) When the plaintiff is suing the United States, its officers or agencies, place an "X" in this box.
Federal question. (3) This refers to suits under 28 U.S.C. 1331, where jurisdiction arises under the Constitution of the United States, an amendment to the Constitution, an act of Congress or a treaty of the United States. In cases where the U.S. is a party, the U.S. plaintiff or defendant code takes precedence, and box 1 or 2 should be marked.
Diversity of citizenship. (4) This refers to suits under 28 U.S.C. 1332, where parties are citizens of different states. When Box 4 is checked, the citizenship of the different parties must be checked. (See Section III below**; NOTE: federal question actions take precedence over diversity cases.**)

III. **Residence (citizenship) of Principal Parties.** This section of the JS 44 is to be completed if diversity of citizenship was indicated above. Mark this section for each principal party.

IV. **Nature of Suit.** Place an "X" in the appropriate box. If there are multiple nature of suit codes associated with the case, pick the nature of suit code that is most applicable. Click here for: Nature of Suit Code Descriptions.

V. **Origin.** Place an "X" in one of the seven boxes.
Original Proceedings. (1) Cases which originate in the United States district courts.
Removed from State Court. (2) Proceedings initiated in state courts may be removed to the district courts under Title 28 U.S.C., Section 1441.
Remanded from Appellate Court. (3) Check this box for cases remanded to the district court for further action. Use the date of remand as the filing date.
Reinstated or Reopened. (4) Check this box for cases reinstated or reopened in the district court. Use the reopening date as the filing date.
Transferred from Another District. (5) For cases transferred under Title 28 U.S.C. Section 1404(a). Do not use this for within district transfers or multidistrict litigation transfers.
Multidistrict Litigation – Transfer. (6) Check this box when a multidistrict case is transferred into the district under authority of Title 28 U.S.C. Section 1407.
Multidistrict Litigation – Direct File. (8) Check this box when a multidistrict case is filed in the same district as the Master MDL docket.
PLEASE NOTE THAT THERE IS NOT AN ORIGIN CODE 7. Origin Code 7 was used for historical records and is no longer relevant due to changes in statute.

VI. **Cause of Action.** Report the civil statute directly related to the cause of action and give a brief description of the cause. **Do not cite jurisdictional statutes unless diversity.** Example: U.S. Civil Statute: 47 USC 553 Brief Description: Unauthorized reception of cable service.

VII. **Requested in Complaint.** Class Action. Place an "X" in this box if you are filing a class action under Rule 23, F.R.Cv.P.
Demand. In this space enter the actual dollar amount being demanded or indicate other demand, such as a preliminary injunction.
Jury Demand. Check the appropriate box to indicate whether or not a jury is being demanded.

VIII. **Related Cases.** This section of the JS 44 is used to reference related pending cases, if any. If there are related pending cases, insert the docket numbers and the corresponding judge names for such cases.

Date and Attorney Signature. Date and sign the civil cover sheet.

UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF PENNSYLVANIA

DESIGNATION FORM
(to be used by counsel to indicate the category of the case for the purpose of assignment to the appropriate calendar)

Address of Plaintiff: 8301 Willow Place Drive N, Apt. 2509, Houston, TX 77070

Address of Defendant: 1 West First Avenue, Conshohocken, PA 19428-1800

Place of Accident, Incident or Transaction: 1 West First Avenue, Conshohocken, PA 19428-1800

RELATED CASE IF ANY:
Case Number: 2:2024-cv-02227 Judge: Cynthia M. Rufe Date Terminated: _____

Civil cases are deemed related when ***Yes*** is answered to any of the following questions:

1. Is this case related to property included in an earlier numbered suit pending or within one year previously terminated action in this court? Yes ☐ No ☒
2. Does this case involve the same issue of fact or grow out of the same transaction as a prior suit Pending or within one year previously terminated action in this court? Yes ☒ No ☐
3. Does this case involve the validity or infringement of a patent already in suit or any earlier Numbered case pending or within one year previously terminated action of this court? Yes ☐ No ☒
4. Is this case a second or successive habeas corpus, social security appeal, or pro se case filed by the same individual? Yes ☐ No ☒

I certify that, to my knowledge, the within case ☐ **is** / ☒ **is not** related to any now pending or within one year previously terminated action in this court except as note above.

DATE: June 12, 2024 _____ PA ID No. 201373

Attorney-at-Law (Must sign above) *Attorney I.D. # (if applicable)*

Civil (Place a √ in one category only)

A. Federal Question Cases:

- ☐ 1. Indemnity Contract, Marine Contract, and All Other Contracts)
- ☐ 2. FELA
- ☐ 3. Jones Act-Personal Injury
- ☐ 4. Antitrust
- ☐ 5. Wage and Hour Class Action/Collective Action
- ☐ 6. Patent
- ☐ 7. Copyright/Trademark
- ☐ 8. Employment
- ☐ 9. Labor-Management Relations
- ☐ 10. Civil Rights
- ☐ 11. Habeas Corpus
- ☐ 12. Securities Cases
- ☐ 13. Social Security Review Cases
- ☐ 14. Qui Tam Cases
- ☐ 15. All Other Federal Question Cases. *(Please specify)*: _____

B. Diversity Jurisdiction Cases:

- ☑ 1. Insurance Contract and Other Contracts
- ☐ 2. Airplane Personal Injury
- ☐ 3. Assault, Defamation
- ☐ 4. Marine Personal Injury
- ☐ 5. Motor Vehicle Personal Injury
- ☐ 6. Other Personal Injury (*Please specify*): _____
- ☐ 7. Products Liability
- ☐ 8. All Other Diversity Cases: *(Please specify)* _____

ARBITRATION CERTIFICATION
(The effect of this certification is to remove the case from eligibility for arbitration)

I, Benjamin F. Johns, counsel of record *or* pro se plaintiff, do hereby certify:

☑ Pursuant to Local Civil Rule 53.2 § 3(c)(2), that to the best of my knowledge and belief, the damages recoverable in this civil action case exceed the sum of $150,000.00 exclusive of interest and costs:

☐ Relief other than monetary damages is sought.

DATE: June 122, 2024 _____ PA ID No. 201373

Attorney-at-Law (Sign here if applicable) *Attorney ID # (if applicable)*

NOTE: A trial de novo will be a jury only if there has been compliance with F.R.C.P. 38.

General Information

Case Name	CASTELLANO v. CENCORA, INC. et al
Court	U.S. District Court for the Eastern District of Pennsylvania
Date Filed	Wed Jun 12 00:00:00 EDT 2024
Federal Nature of Suit	Personal Injury: Other [360]
Docket Number	2:24-cv-02568
Parties	THE LASH GROUP, LLC; CENCORA, INC.; MAURISA CASTELLANO