UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF PENNSYLVANIA

JUAN ANAYA, MARILYN BORNE, DREW DION, KELVIN JAMES, KEVIN MAHLE, KYLE REYNOLDS, VIRGINIA ROMANO, EDWARD SKIBINSKI, CELIA SKORUPSKI, ROBERT ANGULO, TAMI SMITH, SANDRA WEYERMAN, PEYTON MCQUILLEN, MARK HARRELL, MICHELLE PETTIFORD, BONNIE COLLINS-WHITE, JAMES SOWARD, KATELYN SKOWRONSKI, ROBERT MOSKOWITZ, IVERY JOHNSON, THEODORE TSANGARINOS, TUAN NGUYEN, DEBRA BROWN, LISA DESMET, BRIDGET REARDON, MICHAEL WILLIAMSON, AMANDA TUCKER, and MARGIE LOPEZ individually and on behalf of all others similarly situated, Plaintiffs, v. CENCORA, INC. and THE LASH GROUP, LLC, Defendants.	Case No. 2:24-cv-02961-CMR **CONSOLIDATED COMPLAINT – CLASS ACTION** JURY TRIAL DEMANDED

CONSOLIDATED CLASS ACTION COMPLAINT

Plaintiffs Juan Anaya, Marilyn Borne, Drew Dion, Kelvin James, Kevin Mahle, Kyle Reynolds, Virginia Romano, Edward Skibinski, Celia Skorupski, Tami Smith, Robert Angulo, Sandra Weyerman, Peyton McQuillen, Mark Harrell, Michelle Pettiford, Bonnie Collins-White, James Soward, Katelyn Skowronski, Robert Moskowitz, Ivery Johnson, Theodore Tsangarinos, Tuan Nguyen, Debra Brown, Lisa DeSmet, Bridget Reardon, Michael Williamson, Amanda Tucker, and Margie Lopez (collectively, "Plaintiffs"), by and through undersigned counsel, bring

this class action on behalf of themselves and all others similarly situated (the "Class," defined more completely below) against Defendants Cencora, Inc. ("Cencora, Inc.") and The Lash Group, LLC ("Lash Group", and collectively with Cencora, Inc., "Cencora" or "Defendants"). Plaintiffs make the following allegations based on personal knowledge as to their own actions and on information and belief as to all other matters.

NATURE OF THE ACTION

1. Cencora, Inc., formerly known as AmerisourceBergen, is a pharmaceutical giant that brings in over $230 billion in annual revenue. According to Fortune, it was the 24th largest corporation on the planet in 2023 and in 2024 was 10th largest corporation in the United States of America. With over 46,000 employees, Cencora, Inc., its subsidiaries, and affiliates provide services to pharmaceutical companies and pharmacies related to drug distribution, transportation, and logistics, specialty pharmacy, consulting, patient engagement, access, and support, and clinical trial support.[1] Despite its wealth and influence, Cencora and the Lash Group allowed computer hackers to make off with sensitive personal information that, on information and belief, was stored in data systems they jointly used and maintained. This information included, in many cases, intimate medical information, concerning Plaintiffs and millions of Class members.

2. Lash Group, a division of Cencora, Inc., specializes in patient support technologies. Cencora, Inc. and Lash Group work with pharmaceutical firms, healthcare providers, and pharmacies to provide drug distribution, patient access and support services, business analytics, and other services.[2]

[1] *Cencora Reports Fiscal 2024 First Quarter Results*, CENCORA (Jan. 31, 2024), https://investor.cencora.com/financials/quarterly-results/default.aspx.
[2] The Lash Group, https://www.lashgroup.com (last visited Feb. 24, 2025).

3. On February 27, 2024, Cencora, Inc. disclosed in a filing with the U.S. Securities and Exchange Commission ("SEC") that it failed to prevent cybercriminals from infiltrating its systems and stealing sensitive information (the "Data Breach"). The SEC filing confirmed that "[o]n February 21, 2024, Cencora, Inc. [] learned that data from its information systems had been exfiltrated, some of which may contain personal information."[3]

4. Cencora serves more than 18 million patients and handles approximately 20% of the pharmaceuticals distributed across the United States, operating behind the scenes as an agent of many of the world's largest pharmaceutical companies.

5. Cencora has not yet publicly confirmed the total number of individuals, pharmaceutical company partners, or other affiliated divisions or companies that were affected by its Data Breach. Public reports indicate, however, that the Data Breach resulted in the exfiltration of sensitive private information for at least 1.4 million individuals,[4] relating to at least 27 partner pharmaceutical and biotechnology companies[5] as well as other entities related to Cencora.[6]

6. Based on notifications sent to state Attorneys General by Cencora thus far, the list of pharmaceutical companies whose patients', customers', or other affiliated persons' sensitive

[3] Cencora, Inc. (Feb. 27, 2024) *Form 8-K*, available at https://d18rn0p25nwr6d.cloudfront.net/CIK-0001140859/81c828c1-699f-45d0-a610-e985f8e8c4b9.pdf (hereinafter, "*SEC Filing*").
[4] Zack Whittaker, *Pharma giant Cencora is alerting millions about its data breach*, TECHCRUNCH (Aug. 2, 2024), https://techcrunch.com/2024/08/02/pharma-giant-cencora-is-alerting-millions-about-its-data-breach/.
[5] Steve Adler, *Cencora: Additional Data Exfiltrated in February 2024 Cyberattack*, THE HIPAA JOURNAL (Aug. 2, 2024), https://www.hipaajournal.com/cencora-cyberattack-data-breach/.
[6] *See, e.g.*, Steve Adler, *Data Breaches Confirmed by Tri-City Healthcare District; TheraCom*, THE HIPAA JOURNAL (Oct.16, 2024), https://www.hipaajournal.com/data-breach-tri-city-healthcare-district-theracom/ (identifying TheraCom, LLC, which was impacted by the Data Breach, as a Cencora-owned specialty mail-order pharmacy).

personal data was stored by Cencora to administer programs on their behalf and exfiltrated during the breach includes at least: 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 (collectively, "BMS"); Dendreon Pharmaceuticals LLC; Endo Pharmaceuticals Inc.; Genentech, Inc.; GlaxoSmithKline Group of Companies and GlaxoSmithKline Patient Access Programs Foundation (collectively, "GlaxoSmithKline"); Heron Therapeutics, Inc.; Incyte Corporation; Johnson & Johnson Services, Inc.; Johnson & Johnson Patient Assistance Foundation, Inc.; Marathon Pharmaceuticals, LLC/PTC Therapeutics, Inc.; Novartis Pharmaceuticals Corporation ("Novartis"); Otsuka America Pharmaceutical, Inc.; Pfizer Inc. ("Pfizer"); 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 (collectively, the "Drug Companies").[7]

7. Defendants acquire, collect, store, and transfer individuals' sensitive personal data, including personally identifying information ("PII") and protected health information ("PHI") (collectively, "Private Information") on behalf the Drug Companies and other affiliated or partner companies. More specifically, Defendants acquired Plaintiffs' and other Class members' Private Information through the patient engagement, support, and access programs they manage on behalf and under the name of pharmaceutical and similar companies, as well as through other means.

8. Beginning in May and June of 2024, Plaintiffs and Class members learned of the Data Breach for the first time when they received a letter notifying them that their information had been impacted in a Data Breach months prior. The letters indicated that Cencora had learned of the Data Breach on February 21, 2024 and completed its investigation on April 10, 2024. This

[7] *Additional Data Exfiltrated in February 2024 Cyberattack*, n.5, *supra*.

investigation concluded that the stolen information could include names, addresses, dates of birth, health diagnosis information, and medication or prescription information.

9. While letters received by some Plaintiffs and Class members identified the pharmaceutical company on whose behalf Cencora had received and stored individuals' personal information, most of the letters did not disclose the name of the associated pharmaceutical company. Some breach notification letters have specifically identified Drug Companies such as BMS; GlaxoSmithKline; Novartis; and Pfizer; as the companies on whose behalf Cencora administered programs, obtaining and storing Plaintiffs' and Class members' Private Information. The other Drug Companies are referred to in the breach notification letters as "one such organization."

10. Public reports indicate that the Data Breach also resulted in the exfiltration of information from certain Cencora divisions or affiliated companies, including but not limited to World Courier Group, Inc. ("World Courier Group") and Theracom, LLC ("Theracom").

11. World Courier Group, a division of Cencora, is a logistics company with employees in the United States and elsewhere that specializes in transporting temperature-sensitive medical products and provides supply chain management, storage, and other services.

12. In a data breach notification letter dated December 12, 2024, Cencora announced that World Courier Group and certain of its subsidiaries experienced a data breach that involved the personal information of current and former employees, including name, address, data of birth, and Social Security number ("SSN").

13. TheraCom is a "Cencora-owned specialty mail-order pharmacy" and Cencora issued substitute notice that "confirmed that the protected health information of 9,271 individuals

was exfiltrated from its IT systems earlier this year."[8] According to the substitute notice, the exfiltrated files "contained information such as first and last names, addresses, dates of birth, prescription information, medical treatment information, medical histories, health insurance information, medical record numbers, and Medicare/Medicaid numbers."[9] "TheraCom maintained this information for purposes of distribution of prescription medication, often at no charge, to individuals enrolled in patient assistance programs."[10]

14. Thus, Defendants systemically collected and maintained vast amounts of Private Information about millions of individuals. These individuals, including Plaintiffs and Class members, entrusted Defendants with their sensitive data with the mutual understanding that it would be protected against disclosure. Instead, Defendants' negligence has put millions of individuals at lifelong risk of identity theft and fraud.

15. Defendants owed a non-delegable duty to Plaintiffs and Class members to implement reasonable and adequate security measures to protect their Private Information. Yet, Defendants maintained and shared the Private Information in a negligent and/or reckless manner. In particular, Private Information was maintained on computer systems in a condition vulnerable to cyberattacks that lacked, for example, multi-factor authentication to access.

16. After numerous high-profile cyberattacks across the healthcare industry in recent years and numerous warnings by government agencies, such a data breach was a known risk to

---

8 *Data Breaches Confirmed by Tri-City Healthcare District; TheraCom*, n.6, *supra*.

9 *Id.*

10 *TheraCom Pharmacy Substitute Notice of Data Incident to Affected Individuals,* BUSINESSWIRE (Oct. 9, 2024), https://www.businesswire.com/news/home/20241009066663/en/TheraCom-Pharmacy-Substitute-Notice-of-Data-Incident-to-Affected-Individuals.

Defendants. Still, Defendants failed to take the necessary steps to secure Plaintiffs' and Class members' Private Information.

17. Plaintiffs' and Class members' Private Information was compromised due to Defendants' negligent and/or reckless acts and omissions and Defendants' failure to reasonably and adequately protect Plaintiffs' and Class members' Private Information.

18. As a result of the Data Breach, Plaintiffs and Class members suffered concrete injuries in fact including: (i) invasion of privacy; (ii) theft of their Private Information; (iii) fraud and identity theft from the misuse of their stolen Private Information; (iv) lost or diminished value of Private Information; (v) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vi) emotional and mental distress and anguish; (vii) statutory damages; (viii) nominal damages; and (ix) the continued and certainly increased risk to their Private Information, which: (a) remains inadequately secured and vulnerable to unauthorized access and abuse; and (b) remains in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the Private Information.

19. Cybercriminals can (and will) distribute Plaintiffs' and Class members' Private Information from the Data Breach in illicit underground marketplaces, including on the dark web. The information will be used to harm Plaintiffs and Class members in a variety of ways, including: destroying their credit and leaving them financially liable by opening new financial accounts and taking out loans in their names; improperly obtaining or billing for medical services and pharmaceuticals; facilitating other phishing and hacking intrusions, such as through spam emails, texts, and phone calls; impersonating them to obtain benefits; perpetrating medical-related blackmail; and otherwise assuming their identities.

20. As a result of the Data Breach, Plaintiffs and Class members face a substantial and imminent risk of harm relating to the exposure and misuse of their Private Information. Plaintiffs and Class members have and will continue to suffer injuries associated with this risk, including but not limited to a loss of time, mitigation expenses, and anxiety over the misuse of their Private Information.

21. Plaintiffs bring this class action lawsuit individually and on behalf of all those similarly situated to address Defendants' inadequate safeguarding of Class members' Private Information.

22. Further, Plaintiffs and Class members have a continuing interest in ensuring that their information is and remains safe, and they should be entitled to injunctive and other equitable relief.

PARTIES

Plaintiffs

Plaintiff Juan Anaya

23. Plaintiff Juan Anaya is an individual who resides in Tinley Park, Illinois.

24. Plaintiff Anaya participated in a patient support program and/or otherwise received healthcare, pharmaceuticals, or pharmaceutical related services from GlaxoSmithKline, which engaged Cencora and Lash Group to assist in providing those healthcare or pharmaceutical related services, including by collecting Plaintiff Anaya's information on GlaxoSmithKline's behalf.

25. As a condition of participating in the patient support program and/or otherwise receiving healthcare or pharmaceutical related services, Plaintiff Anaya provided Private Information either to GlaxoSmithKline directly, Cencora directly at the request of GlaxoSmithKline, or to his healthcare providers or pharmacies which provided that information

to GlaxoSmithKline and/or Cencora indirectly.

26. Plaintiff Anaya's health, treatment, healthcare provider, prescriptions, and other information related to his health care is highly private, and Plaintiff values that privacy. The release of that private information risks not only identity theft and/or fraud, among other similar harms, but also related harms such as the embarrassment, harassment, and discrimination that can result from release of private healthcare information.

27. Plaintiff Anaya has a private medical condition for which he seeks medical care and the treatment of which requires one or more pharmaceutical drugs, which is highly private information. The privacy of Plaintiff Anaya's health, treatment, healthcare provider, prescriptions, and other information related to his health care is important to Plaintiff Anaya. The release of that information risks not only identity theft and/or fraud, among other similar harms, but also related harms such as the embarrassment, harassment, and discrimination that can result from release of private healthcare information.

28. Plaintiff Anaya received a letter from Cencora dated May 24, 2024, notifying him that the Data Breach had impacted his Private Information, which Cencora had obtained either directly from GlaxoSmithKline, or on behalf of GlaxoSmithKline, or from some other source.

29. In the letter, Cencora disclosed that the following Private Information of Plaintiff may have been disclosed during the Data Breach: name, address, date of birth, health diagnosis, and/or medications and prescriptions. The letter identified that Plaintiff's Private Information was in Lash Group's possession through patient support and access programs that it manages on behalf of GlaxoSmithKline.

30. Cencora obtained or received, and continues to store and maintain, Plaintiff Anaya's Private Information. Cencora owed and owes Plaintiff Anaya a legal duty and obligation

to protect his Private Information from unauthorized access and disclosure. Plaintiff Anaya's Private information was compromised and disclosed as a result of Cencora's inadequate data security practices, which resulted in the Data Breach.

31. Plaintiff Anaya is very careful with his Private Information. Plaintiff Anaya either stores documents containing Private Information in a safe and secure location, or destroys the documents. Plaintiff Anaya would not have entrusted his Private Information to GlaxoSmithKline and/or Cencora, or otherwise would not have permitted his Private Information to be provided to GlaxoSmithKline and Cencora, had he known that Cencora maintains lax data security practices and is susceptible to data disclosures and privacy violations.

32. In response to the Data Breach, Plaintiff Anaya diligently undertook measures to mitigate its effects, including monitoring his accounts for suspicious activity; changing his passwords; and reviewing his information on Credit Karma. He has invested considerable time addressing the fallout of the breach – time that would have otherwise been allocated to work or leisure activities. Regrettably, the time is irretrievably lost and cannot be reclaimed.

33. Plaintiff Anaya has also experienced attempted fraud since the occurrence of the Data Breach, including attempted fraud on one of his financial accounts; and a significant increase in suspicious spam calls, texts, and emails.

34. Plaintiff Anaya has suffered tangible harm resulting from the compromise of his Private Information due to the Data Breach, including, but not limited to: (i) an invasion of privacy; (ii) the unlawful appropriation of Private Information; (iii) a reduction or loss in the value of Private Information; (iv) expended time and lost opportunity costs incurred in mitigating the actual repercussions of the Data Breach; (v) statutory damages; (vi) nominal damages; and (vii)

the enduring and potentially escalating exposure of his Private Information to risk of unauthorized access and misuse by third parties.

35. The Data Breach has caused Plaintiff Anaya to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendants have still not fully informed him of key details about the Data Breach's occurrence.

36. As a result of the Data Breach, Plaintiff Anaya anticipates spending time and resources in the future to try to mitigate and address harms caused by the Data Breach.

37. As a result of the Data Breach, Plaintiff Anaya is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

38. Plaintiff Anaya has a continuing interest in ensuring that his Private Information, which remains in Defendants' possession, is protected and safeguarded from future breaches.

Plaintiff Marilyn Borne

39. Plaintiff Marilyn Borne is an individual who resides in Walker Lake, Louisiana.

40. Plaintiff Borne participated in a patient support program and/or otherwise received healthcare, pharmaceuticals, or pharmaceutical related services from BMS, which engaged Cencora and Lash Group to assist in providing those healthcare or pharmaceutical related services, including by collecting Borne's information on BMS's behalf.

41. As a condition of participating in the patient support program and/or otherwise receiving healthcare or pharmaceutical related services, Plaintiff Borne provided Private Information either to BMS directly, Cencora directly at the request of BMS, or to her healthcare providers or pharmacies which provided that information to BMS and/or Cencora indirectly.

42. Plaintiff Borne's health, treatment, healthcare provider, prescriptions, and other information related to her health care is highly private, and Plaintiff values that privacy. The

release of that private information risks not only identity theft and/or fraud, among other similar harms, but also related harms such as the embarrassment, harassment, and discrimination that can result from release of private healthcare information.

43. Plaintiff Borne has a private medical condition for which she seeks medical care and the treatment of which requires one or more pharmaceutical drugs, which is highly private information. The privacy of Plaintiff Borne's health, treatment, healthcare provider, prescriptions, and other information related to her health care is important to Plaintiff Borne. The release of that information risks not only identity theft and/or fraud, among other similar harms, but also related harms such as the embarrassment, harassment, and discrimination that can result from release of private healthcare information.

44. Plaintiff Borne received a letter from Cencora dated May 17, 2024, notifying her that the Data Breach had impacted her Private Information, which Cencora had obtained either directly from BMS, or on behalf of BMS, or from some other source.

45. In the letter, Cencora disclosed that the following Private Information of Plaintiff may have been disclosed during the Data Breach: name, address, date of birth, health diagnosis, and/or medications and prescriptions. The letter identified that Plaintiff's Private Information was in Lash Group's possession through patient support and access programs that it manages on behalf of BMS.

46. Cencora obtained or received, and continues to store and maintain, Plaintiff Borne's Private Information. Cencora owed and owes Plaintiff Borne a legal duty and obligation to protect her Private Information from unauthorized access and disclosure. Plaintiff Borne's Private Information was compromised and disclosed as a result of Cencora's inadequate data security practices, which resulted in the Data Breach.

47. Plaintiff Borne is very careful with her Private Information. Plaintiff Borne either stores documents containing Private Information in a safe and secure location, or destroys the documents. Plaintiff Borne would not have entrusted her Private Information to BMS and/or Cencora, or otherwise would not have permitted her Private Information to be provided to BMS and Cencora, had she known that Cencora maintains lax data security practices and is susceptible to data disclosures and privacy violations.

48. In response to the Data Breach, Plaintiff Borne diligently undertook measures to mitigate its effects, including researching the Data Breach; placing a freeze on her credit at all three bureaus; monitoring her accounts for suspicious activity; changing her passwords; and obtaining a replacement debit card. She has invested considerable time addressing the fallout of the breach – time that would have otherwise been allocated to work or leisure activities. Regrettably, the time is irretrievably lost and cannot be reclaimed.

49. Plaintiff Borne has also experienced attempted fraud since the occurrence of the Data Breach, including a significant increase in suspicious spam and phishing emails.

50. Plaintiff Borne has suffered tangible harm resulting from the compromise of her Private Information due to the Data Breach, including, but not limited to: (i) an invasion of privacy; (ii) the unlawful appropriation of Private Information; (iii) a reduction or loss in the value of Private Information; (iv) expended time and lost opportunity costs incurred in mitigating the actual repercussions of the Data Breach; (v) statutory damages; (vi) nominal damages; and (vii) the enduring and potentially escalating exposure of her Private Information to risk of unauthorized access and misuse by third parties.

51. The Data Breach has caused Plaintiff Borne to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendants have still not fully informed her of key

details about the Data Breach's occurrence.

52. As a result of the Data Breach, Plaintiff Borne anticipates spending time and resources in the future to try to mitigate and address harms caused by the Data Breach.

53. As a result of the Data Breach, Plaintiff Borne is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

54. Plaintiff Borne has a continuing interest in ensuring that her Private Information, which remains in Defendants' possession, is protected and safeguarded from future breaches.

Plaintiff Drew Dion

55. Plaintiff Drew Dion is an individual who resides in Surprise, Arizona.

56. Plaintiff Dion's health, treatment, healthcare provider, prescriptions, and other information related to his health care is highly private, and Plaintiff values that privacy. The release of that private information risks not only identity theft and/or fraud, among other similar harms, but also related harms such as the embarrassment, harassment, and discrimination that can result from release of private healthcare information.

57. Plaintiff Dion received a letter from Cencora dated May 28, 2024, notifying him that the Data Breach had impacted his Private Information, which Cencora had obtained through "one . . . organization in connection with its patient support programs."

58. In the letter, Cencora disclosed that the following Private Information of Plaintiff may have been disclosed during the Data Breach: name, address, date of birth, health diagnosis, and/or medications and prescriptions. The letter identified that Plaintiff's Private Information was in Lash Group's possession through its partnership with "one . . . organization in connection with its patient support programs."

59. Cencora obtained or received, and continues to store and maintain, Plaintiff Dion's Private Information. Cencora owed and owes Plaintiff Dion a legal duty and obligation to protect his Private Information from unauthorized access and disclosure. Plaintiff Dion's Private Information was compromised and disclosed as a result of Cencora's inadequate data security practices, which resulted in the Data Breach.

60. Plaintiff Dion is very careful with his Private Information. Plaintiff Dion either stores documents containing Private Information in a safe and secure location, or destroys the documents. Plaintiff Dion would not have entrusted his Private Information to Cencora, or otherwise would not have permitted his Private Information to be provided to Cencora, had he known that Cencora maintains lax data security practices and is susceptible to data disclosures and privacy violations.

61. In response to the Data Breach, Plaintiff Dion diligently undertook measures to mitigate its effects. This included purchasing Norton identity theft services; researching the Data Breach; reviewing and monitoring his credit report and financial accounts; changing his passwords; and communicating with his bank regarding attempted fraud. He has invested considerable time addressing the fallout of the breach – time that would have otherwise been allocated to work or leisure activities. Regrettably, the time is irretrievably lost and cannot be reclaimed.

62. Plaintiff Dion has also experienced attempted fraud since the occurrence of the Data Breach, including a fraudulent charge on one of his financial accounts; unfamiliar credit inquiries on his credit report; notifications from Norton that his personal information is available on the dark web; and a significant increase in suspicious spam calls and texts.

63. Plaintiff Dion has suffered tangible harm resulting from the compromise of his Private Information due to the Data Breach, including, but not limited to: (i) an invasion of privacy; (ii) the unlawful appropriation of Private Information; (iii) a reduction or loss in the value of Private Information; (iv) expended time and opportunity costs incurred in mitigating the actual repercussions of the Data Breach; (v) statutory damages; (vi) nominal damages; and (vii) the enduring and potentially escalating exposure of his Private Information to risk of unauthorized access and misuse by third parties.

64. The Data Breach has caused Plaintiff Dion to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendants have still not fully informed him of key details about the Data Breach's occurrence.

65. As a result of the Data Breach, Plaintiff Dion anticipates spending time and resources in the future to try to mitigate and address harms caused by the Data Breach.

66. As a result of the Data Breach, Plaintiff Dion is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

67. Plaintiff Dion has a continuing interest in ensuring that his Private Information, which remains in Defendants' possession, is protected and safeguarded from future breaches.

Plaintiff Kelvin James

68. Plaintiff Kelvin James is an individual who resides in Auburn, Alabama.

69. Plaintiff James participated in a patient support program and/or otherwise received healthcare, pharmaceuticals, or pharmaceutical related services from BMS, which engaged Cencora and Lash Group to assist in providing those healthcare or pharmaceutical related services, including by collecting James' information on BMS's behalf.

70. As a condition of participating in the patient support program and/or otherwise receiving healthcare or pharmaceutical related services, Plaintiff James provided Private Information either to BMS directly, Cencora directly at the request of BMS, or to his healthcare providers or pharmacies which provided that information BMS and/or Cencora indirectly.

71. Plaintiff James' health, treatment, healthcare provider, prescriptions, and other information related to his health care is highly private, and Plaintiff values that privacy. The release of that private information risks not only identity theft and/or fraud, among other similar harms, but also related harms such as the embarrassment, harassment, and discrimination that can result from release of private healthcare information.

72. Plaintiff James has a private medical condition for which he seeks medical care and the treatment of which requires one or more pharmaceutical drugs, which is highly private information. The privacy of Plaintiff James' health, treatment, healthcare provider, prescriptions, and other information related to his health care is important to Plaintiff James. The release of that information risks not only identity theft and/or fraud, among other similar harms, but also related harms such as the embarrassment, harassment, and discrimination that can result from release of private healthcare information.

73. Plaintiff James received a letter from Cencora dated May 17, 2024, notifying him that the Data Breach had impacted his Private Information, which Cencora had obtained either directly from BMS, or on behalf of BMS, or from some other source.

74. In the letter, Cencora disclosed that the following Private Information of Plaintiff may have been disclosed during the Data Breach: name, address, date of birth, health diagnosis, and/or medications and prescriptions. The letter identified that Plaintiff's Private Information was

in Lash Group's possession through patient support and access programs that it manages on behalf of BMS.

75. Cencora obtained or received, and continues to store and maintain Plaintiff James' Private Information. Cencora owed and owes Plaintiff James a legal duty and obligation to protect his Private Information from unauthorized access and disclosure. Plaintiff James' Private Information was compromised and disclosed as a result of Cencora's inadequate data security practices, which resulted in the Data Breach.

76. Plaintiff James is very careful with his Private Information. Plaintiff James either stores documents containing Private Information in a safe and secure location, or destroys the documents. Plaintiff James would not have entrusted his Private Information to BMS and/or Cencora, or otherwise would not have permitted his Private Information to be provided to BMS and Cencora, had he known that Cencora maintains lax data security practices and is susceptible to data disclosures and privacy violations.

77. In response to the Data Breach, Plaintiff James diligently undertook measures to mitigate its effects, including researching the Data Breach; monitoring his accounts for suspicious activity; changing his account passwords; and requesting replacement cards. He has invested considerable time addressing the fallout of the breach – time that would have otherwise been allocated to work or leisure activities. Regrettably, the time is irretrievably lost and cannot be reclaimed.

78. Plaintiff James has also experienced actual and attempted fraud since the occurrence of the Data Breach, including fraudulent attempts on his checking account; and inquiries on his credit that he does not recognize. Further, in or around September 2024, an

individual made fraudulent charges to Plaintiff James' account for a total of approximately $5900. That fraudulent charge is still outstanding and has not been refunded or otherwise resolved.

79. Plaintiff James has suffered tangible harm resulting from the compromise of his Private Information due to the Data Breach, including, but not limited to: (i) an invasion of privacy; (ii) the unlawful appropriation of Private Information; (iii) a reduction or loss in the value of Private Information; (iv) expended time and opportunity costs incurred in mitigating the actual repercussions of the Data Breach; (v) statutory damages; (vi) nominal damages; and (vii) the enduring and potentially escalating exposure of his Private Information to risk of unauthorized access and misuse by third parties.

80. The Data Breach has caused Plaintiff James to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendants have still not fully informed him of key details about the Data Breach's occurrence.

81. As a result of the Data Breach, Plaintiff James anticipates spending time and resources in the future to try to mitigate and address harms caused by the Data Breach.

82. As a result of the Data Breach, Plaintiff James is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

83. Plaintiff James has a continuing interest in ensuring that his Private Information, which remains in Defendants' possession, is protected and safeguarded from future breaches.

Plaintiff Kevin Mahle

84. Plaintiff Mahle is an individual who resides in Havre, Montana.

85. Plaintiff Mahle's health, treatment, healthcare provider, prescriptions, and other information related to his health care is highly private, and Plaintiff values that privacy. The release of that private information risks not only identity theft and/or fraud, among other similar

harms, but also related harms such as the embarrassment, harassment, and discrimination that can result from release of private healthcare information.

86. Plaintiff Mahle received a letter from Cencora dated May 21, 2024, notifying him that the Data Breach had impacted his/ Private Information, which Cencora had obtained through "one . . . organization in connection with its patient support programs."

87. In the letter, Cencora disclosed that the following Private Information of Plaintiff may have been disclosed during the Data Breach: name, address, date of birth, health diagnosis and/or medications and prescriptions. The letter identified that Plaintiff's Private Information was in Lash Group's possession through its partnership with "one . . . organization in connection with its patient support programs."

88. Cencora obtained or received, and continues to store and maintain Plaintiff Mahle's Private Information. Cencora owed and owes Plaintiff Mahle a legal duty and obligation to protect his Private Information from unauthorized access and disclosure. Plaintiff Mahle's Private Information was compromised and disclosed as a result of Cencora's inadequate data security practices, which resulted in the Data Breach.

89. Plaintiff Mahle is very careful with his Private Information. Plaintiff Mahle either stores documents containing Private Information in a safe and secure location, or destroys the documents. Plaintiff Mahle would not have entrusted his Private Information to Cencora, or otherwise would not have permitted his Private Information to be provided to Cencora, had he known that Cencora maintains lax data security practices and is susceptible to data disclosures and privacy violations.

90. In response to the Data Breach, Plaintiff Mahle diligently undertook measures to mitigate its effects, including dealing with fraud resulting from the Data Breach, researching the

Data Breach, monitoring his financial accounts, and changing his passwords. He has invested considerable time addressing the fallout of the breach – time that would have otherwise been allocated to work or leisure activities. Regrettably, the time is irretrievably lost and cannot be reclaimed.

91. Plaintiff Mahle has also experienced actual and attempted fraud since the occurrence of the Data Breach, including fraudulent charges on his credit card; credit card applications opened in his name; a checking account opened in his name in Hawaii; and an application for unemployment under his name. In addition, an individual attempted to obtain a business refund from the IRS in Plaintiff Mahle's name in July 2024. This attempted IRS fraud is currently unresolved.

92. Plaintiff Mahle has suffered tangible harm resulting from the compromise of his Private Information due to the Data Breach, including, but not limited to: (i) an invasion of privacy; (ii) the unlawful appropriation of Private Information; (iii) a reduction or loss in the value of Private Information; (iv) expended time and lost opportunity costs incurred in mitigating the actual repercussions of the Data Breach; (v) statutory damages; (vi) nominal damages; and (vii) the enduring and potentially escalating exposure of his Private Information to risk of unauthorized access and misuse by third parties.

93. The Data Breach has caused Plaintiff Mahle to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendants have still not fully informed him of key details about the Data Breach's occurrence.

94. As a result of the Data Breach, Plaintiff Mahle anticipates spending time and resources in the future to try to mitigate and address harms caused by the Data Breach.

95. As a result of the Data Breach, Plaintiff Mahle is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

96. Plaintiff Mahle has a continuing interest in ensuring that his Private Information, which remains in Defendants' possession, is protected and safeguarded from future breaches.

Plaintiff Kyle Reynolds

97. Plaintiff Kyle Reynolds is an individual who resides in Charlotte, North Carolina.

98. Plaintiff Reynolds' health, treatment, healthcare provider, prescriptions, and other information related to his health care is highly private, and Plaintiff values that privacy. The release of that private information risks not only identity theft and/or fraud, among other similar harms, but also related harms such as the embarrassment, harassment, and discrimination that can result from release of private healthcare information.

99. Plaintiff Reynolds received a letter from Cencora dated May 30, 2024, notifying him that the Data Breach had impacted his Private Information, which Cencora had obtained through "one . . . organization in connection with its patient support programs."

100. In the letter, Cencora disclosed that the following Private Information of Plaintiff may have been disclosed during the Data Breach: name, address, date of birth, health diagnosis, and/or medications and prescriptions. The letter identified that Plaintiff's Private Information was in Lash Group's possession through patient support and access programs that it manages on behalf of "one . . . organization in connection with its patient support programs."

101. Cencora obtained or received, and continues to store and maintain, Plaintiff Reynolds's Private Information. Cencora owed and owes Plaintiff Reynolds a legal duty and obligation to protect his Private Information from unauthorized access and disclosure. Plaintiff

Reynolds's Private Information was compromised and disclosed as a result of Cencora's inadequate data security practices, which resulted in the Data Breach.

102. Plaintiff Reynolds is very careful with his Private Information. Plaintiff Reynolds either stores documents containing Private Information in a safe and secure location, or destroys the documents. Plaintiff Reynolds would not have entrusted his Private Information to Cencora, or otherwise would not have permitted his Private Information to be provided to Cencora, had he known that Cencora maintains lax data security practices and is susceptible to data disclosures and privacy violations.

103. In response to the Data Breach, Plaintiff Reynolds diligently undertook measures to mitigate its effects, including placing a credit alert and freeze with all three bureaus and communicating with his bank regarding fraudulent charges. He has invested considerable time addressing the fallout of the breach – time that would have otherwise been allocated to work or leisure activities. Regrettably, the time is irretrievably lost and cannot be reclaimed.

104. Plaintiff Reynolds has also experienced attempted fraud since the occurrence of the Data Breach, including a fraudulent attempt to open a new banking account in his name; and a significant increase in suspicious calls, texts, and emails.

105. Plaintiff Reynolds has suffered tangible harm resulting from the compromise of his Private Information due to the Data Breach, including, but not limited to: (i) an invasion of privacy; (ii) the unlawful appropriation of Private Information; (iii) a reduction or loss in the value of Private Information; (iv) expended time and lost opportunity costs incurred in mitigating the actual repercussions of the Data Breach; (v) statutory damages; (vi) nominal damages; and (vii) the enduring and potentially escalating exposure of his Private Information to risk of unauthorized access and misuse by third parties.

106. The Data Breach has caused Plaintiff Reynolds to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendants have still not fully informed him of key details about the Data Breach's occurrence.

107. As a result of the Data Breach, Plaintiff Reynolds anticipates spending time and resources in the future to try to mitigate and address harms caused by the Data Breach.

108. As a result of the Data Breach, Plaintiff Reynolds is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

109. Plaintiff Reynolds has a continuing interest in ensuring that his Private Information, which remains in Defendants' possession, is protected and safeguarded from future breaches.

Plaintiff Virginia Romano

110. Plaintiff Virginia Romano is an individual who resides in Elkhart, Indiana.

111. Plaintiff Romano's health, treatment, healthcare provider, prescriptions, and other information related to her health care is highly private, and Plaintiff values that privacy. The release of that private information risks not only identity theft and/or fraud, among other similar harms, but also related harms such as the embarrassment, harassment, and discrimination that can result from release of private healthcare information.

112. Plaintiff Romano received a letter from Cencora dated May 30, 2024, notifying her that the Data Breach had impacted her Private Information, which Cencora had obtained through "one . . . organization in connection with its patient support programs."

113. In the letter, Cencora disclosed that the following Private Information of Plaintiff may have been disclosed during the Data Breach: name, address, date of birth, health diagnosis, and/or medications and prescriptions. The letter identified that Plaintiff's Private Information was

in Lash Group's possession through patient support and access programs that it manages on behalf of "one . . . organization in connection with its patient support programs."

114. Cencora obtained or received, and continues to store and maintain, Plaintiff Romano's Private Information. Cencora owed and owes Plaintiff Romano a legal duty and obligation to protect her Private Information from unauthorized access and disclosure. Plaintiff Romano's Private Information was compromised and disclosed as a result of Cencora's inadequate data security practices, which resulted in the Data Breach.

115. Plaintiff Romano is very careful with her Private Information. Plaintiff Romano either stores documents containing Private Information, or destroys the documents. Plaintiff Romano would not have entrusted her Private Information to Cencora, or otherwise would not have permitted her Private Information to be provided to Cencora, had she known that Cencora maintains lax data security practices and is susceptible to data disclosures and privacy violations.

116. In response to the Data Breach, Plaintiff Romano diligently undertook measures to mitigate its effects, including placing a freeze on her credit at all three bureaus; monitoring her accounts for suspicious activity; changing her passwords; and speaking with her bank regarding fraud and obtaining new cards. She has invested considerable time addressing the fallout of the breach – time that would have otherwise been allocated to work or leisure activities. Regrettably, the time is irretrievably lost and cannot be reclaimed.

117. Plaintiff Romano has also experienced attempted fraud since the occurrence of the Data Breach, including various fraudulent charges on her bank accounts; and an increase in suspicious spam calls and texts.

118. Plaintiff Romano has suffered tangible harm resulting from the compromise of her Private Information due to the Data Breach, including, but not limited to: (i) an invasion of

privacy; (ii) the unlawful appropriation of Private Information; (iii) a reduction or loss in the value of Private Information; (iv) expended time and opportunity costs incurred in mitigating the actual repercussions of the Data Breach; (v) statutory damages; (vi) nominal damages; and (vii) the enduring and potentially escalating exposure of her Private Information to risk of unauthorized access and misuse by third parties.

119. The Data Breach has caused Plaintiff Romano to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendants have still not fully informed her of key details about the Data Breach's occurrence.

120. As a result of the Data Breach, Plaintiff Romano anticipates spending time and resources in the future to try to mitigate and address harms caused by the Data Breach.

121. As a result of the Data Breach, Plaintiff Romano is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

122. Plaintiff Romano has a continuing interest in ensuring that her Private Information, which remains in Defendants' possession, is protected and safeguarded from future breaches.

Plaintiff Edward Skibinski

123. Plaintiff Edward Skibinski is an individual who resides in Royersford, Pennsylvania.

124. Plaintiff Skibinski's health, treatment, healthcare provider, prescriptions, and other information related to his health care is highly private, and Plaintiff values that privacy. The release of that private information risks not only identity theft and/or fraud, among other similar harms, but also related harms such as the embarrassment, harassment, and discrimination that can result from release of private healthcare information.

125. Plaintiff Skibinski received a letter from Cencora dated May 22, 2024, notifying him that the Data Breach had impacted his Private Information, which Cencora had obtained through "one . . . organization in connection with its patient support programs."

126. In the letter, Cencora disclosed that the following Private Information of Plaintiff may have been disclosed during the Data Breach: name, address, date of birth, health diagnosis, and/or medications and prescriptions. The letter identified that Plaintiff's Private Information was in Lash Group's possession through patient support and access programs that it manages on behalf of "one . . . organization in connection with its patient support programs."

127. Cencora obtained or received, and continues to store and maintain, Plaintiff Skibinski's Private Information. Cencora owed and owes Plaintiff Skibinski a legal duty and obligation to protect his Private Information from unauthorized access and disclosure. Plaintiff Skibinski's Private Information was compromised and disclosed as a result of Cencora's inadequate data security practices, which resulted in the Data Breach.

128. Plaintiff Skibinski is very careful with his Private Information. Plaintiff Skibinski either stores documents containing Private Information in a safe and secure location, or destroys the documents. Plaintiff Skibinski would not have entrusted his Private Information to Cencora, or otherwise would not have permitted his Private Information to be provided to Cencora, had he known that Cencora maintains lax data security practices and is susceptible to data disclosures and privacy violations.

129. In response to the Data Breach, Plaintiff Skibinski diligently undertook measures to mitigate its effects, including monitoring his accounts for suspicious activity. He has invested considerable time addressing the fallout of the breach – time that would have otherwise been

allocated to work or leisure activities. Regrettably, the time is irretrievably lost and cannot be reclaimed.

130. Plaintiff Skibinski has also experienced attempted fraud since the occurrence of the Data Breach, including an increase in suspicious and spam calls, texts, and emails.

131. Plaintiff Skibinski has suffered tangible harm resulting from the compromise of his Private Information due to the Data Breach, including, but not limited to: (i) an invasion of privacy; (ii) the unlawful appropriation of Private Information; (iii) a reduction or loss in the value of Private Information; (iv) expended time and lost opportunity costs incurred in mitigating the actual repercussions of the Data Breach; (v) statutory damages; (vi) nominal damages; and (vii) the enduring and potentially escalating exposure of his Private Information to risk of unauthorized access and misuse by third parties.

132. The Data Breach has caused Plaintiff Skibinski to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendants have still not fully informed him of key details about the Data Breach's occurrence.

133. As a result of the Data Breach, Plaintiff Skibinski anticipates spending time and resources in the future to try to mitigate and address harms caused by the Data Breach.

134. As a result of the Data Breach, Plaintiff Skibinski is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

135. Plaintiff Skibinski has a continuing interest in ensuring that his Private Information, which remains in Defendants' possession, is protected and safeguarded from future breaches.

Plaintiff Celia Skorupski

136. Plaintiff Celia Skorupski is an individual who resides in Bristol, Connecticut.

137. Plaintiff Skorupski's health, treatment, healthcare provider, prescriptions, and other information related to her health care is highly private, and Plaintiff values that privacy. The release of that private information risks not only identity theft and/or fraud, among other similar harms, but also related harms such as the embarrassment, harassment, and discrimination that can result from release of private healthcare information.

138. Plaintiff Skorupski received a letter from Cencora dated May 21, 2024, notifying her that the Data Breach had impacted her Private Information, which Cencora had obtained through "one . . . organization in connection with its patient support programs."

139. In the letter, Cencora disclosed that the following Private Information of Plaintiff may have been disclosed during the Data Breach: name, address, date of birth, health diagnosis, and/or medications and prescriptions. The letter identified that Plaintiff's Private Information was in Lash Group's possession through patient support and access programs that it manages on behalf of "one . . . organization in connection with its patient support programs."

140. Cencora obtained or received, and continues to store and maintain, Plaintiff Skorupski's Private Information. Cencora owed and owes Plaintiff Skorupski a legal duty and obligation to protect her Private Information from unauthorized access and disclosure. Plaintiff Skorupski's Private Information was compromised and disclosed as a result of Cencora's inadequate data security practices, which resulted in the Data Breach.

141. Plaintiff Skorupski is very careful with her Private Information. Plaintiff Skorupski either stores documents containing Private Information in a safe and secure location, or destroys the documents. Plaintiff Skorupski would not have entrusted her Private Information to Cencora, or otherwise would not have permitted her Private Information to be provided to

Cencora, had she known that Cencora maintains lax data security practices and is susceptible to data disclosures and privacy violations.

142. In response to the Data Breach, Plaintiff Skorupski diligently undertook measures to mitigate its effects, including researching the Data Breach; monitoring her accounts for suspicious activity; and changing her passwords. She has invested considerable time addressing the fallout of the breach – time that would have otherwise been allocated to work or leisure activities. Regrettably, the time is irretrievably lost and cannot be reclaimed.

143. Plaintiff Skorupski has also experienced attempted fraud since the occurrence of the Data Breach, including a significant increase in suspicious spam calls, emails, and texts; and notifications that her personal information is available on the dark web.

144. Plaintiff Skorupski has suffered tangible harm resulting from the compromise of her Private Information due to the Data Breach, including, but not limited to: (i) an invasion of privacy; (ii) the unlawful appropriation of Private Information; (iii) a reduction or loss in the value of Private Information; (iv) expended time and lost opportunity costs incurred in mitigating the actual repercussions of the Data Breach; (v) statutory damages; (vi) nominal damages; and (vii) the enduring and potentially escalating exposure of her Private Information to risk of unauthorized access and misuse by third parties.

145. The Data Breach has caused Plaintiff Skorupski to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendants have still not fully informed her of key details about the Data Breach's occurrence.

146. As a result of the Data Breach, Plaintiff Skorupski anticipates spending time and resources in the future to try to mitigate and address harms caused by the Data Breach.

147. As a result of the Data Breach, Plaintiff Skorupski is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

148. Plaintiff Skorupski has a continuing interest in ensuring that her Private Information, which remains in Defendants' possession, is protected and safeguarded from future breaches.

Plaintiff Tami Smith

149. Plaintiff Tami Smith is an individual who resides in Cabot, Arkansas.

150. Plaintiff Smith's health, treatment, healthcare provider, prescriptions, and other information related to her health care is highly private, and Plaintiff values that privacy. The release of that private information risks not only identity theft and/or fraud, among other similar harms, but also related harms such as the embarrassment, harassment, and discrimination that can result from release of private healthcare information.

151. Plaintiff Smith received a letter from Cencora dated May 21, 2024, notifying her that the Data Breach had impacted her Private Information, which Cencora had obtained through "one . . . organization in connection with its patient support programs."

152. In the letter, Cencora disclosed that the following Private Information of Plaintiff may have been disclosed during the Data Breach: name, address date of birth, health diagnosis and/or medications and prescriptions. The letter identified that Plaintiff's Private Information was in Lash Group's possession through patient support and access programs that it manages on behalf of "one . . . organization in connection with its patient support programs."

153. Cencora obtained or received, and continues to store and maintain, Plaintiff Smith's Private Information. Cencora owed and owes Plaintiff Smith a legal duty and obligation to protect her Private Information from unauthorized access and disclosure. Plaintiff Smith's

Private Information was compromised and disclosed as a result of Cencora's inadequate data security practices, which resulted in the Data Breach.

154. Plaintiff Smith is very careful with her Private Information. Plaintiff Smith either stores documents containing Private Information in a safe and secure location, or destroys the documents. Plaintiff Smith would not have entrusted her Private Information to Cencora, or otherwise would not have permitted her Private Information to be provided to Cencora, had she known that Cencora maintains lax data security practices and is susceptible to data disclosures and privacy violations.

155. In response to the Data Breach, Plaintiff Smith diligently undertook measures to mitigate its effects, including monitoring her financial accounts for suspicious activity; and addressing attempted fraud on her checking account/obtaining a new payment card. She has invested considerable time addressing the fallout of the breach – time that would have otherwise been allocated to work or leisure activities. Regrettably, the time is irretrievably lost and cannot be reclaimed.

156. Plaintiff Smith has also experienced attempted fraud since the occurrence of the Data Breach, including a fraudulent attempt to take cash out of her checking account.

157. Plaintiff Smith has suffered tangible harm resulting from the compromise of her Private Information due to the Data Breach, including, but not limited to: (i) an invasion of privacy; (ii) the unlawful appropriation of Private Information; (iii) a reduction or loss in the value of Private Information; (iv) expended time and lost opportunity costs incurred in mitigating the actual repercussions of the Data Breach; (v) statutory damages; (vi) nominal damages; and (vii) the enduring and potentially escalating exposure of her Private Information to risk of unauthorized access and misuse by third parties.

158. The Data Breach has caused Plaintiff Smith to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendants have still not fully informed her of key details about the Data Breach's occurrence.

159. As a result of the Data Breach, Plaintiff Smith anticipates spending time and resources in the future to try to mitigate and address harms caused by the Data Breach.

160. As a result of the Data Breach, Plaintiff Smith is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

161. Plaintiff Smith has a continuing interest in ensuring that her Private Information, which remains in Defendants' possession, is protected and safeguarded from future breaches.

Plaintiff Robert Angulo

162. Plaintiff Robert Angulo is an individual who resides in Chicago, Illinois.

163. Plaintiff Angulo participated in a patient support program and/or otherwise received healthcare, pharmaceuticals, or pharmaceutical related services from GlaxoSmithKline, which engaged Cencora and Lash Group to assist in providing those healthcare or pharmaceutical related services, including by collecting Plaintiff Angulo's information on GlaxoSmithKine's behalf.

164. As a condition of participating in the patient support program and/or otherwise receiving healthcare or pharmaceutical related services, Plaintiff Angulo provided Private Information either to GlaxoSmithKline directly, Cencora directly at the request of GlaxoSmithKline, or to his healthcare providers or pharmacies which provided that information GlaxoSmithKline and/or Cencora indirectly.

165. Plaintiff Angulo's health, treatment, healthcare provider, prescriptions, and other information related to his health care is highly private, and Plaintiff values that privacy. The

release of that private information risks not only identity theft and/or fraud, among other similar harms, but also related harms such as the embarrassment, harassment, and discrimination that can result from release of private healthcare information.

166. Plaintiff Angulo has a private medical condition for which he seeks medical care and the treatment of which requires one or more pharmaceutical drugs, which is highly private information. The privacy of Plaintiff Angulo's health, treatment, healthcare provider, prescriptions, and other information related to his health care is important to Plaintiff Angulo. The release of that information risks not only identity theft and/or fraud, among other similar harms, but also related harms such as the embarrassment, harassment, and discrimination that can result from release of private healthcare information.

167. Plaintiff Angulo received a letter from Cencora dated May 24, 2024, notifying him that the Data Breach had impacted his Private Information, which Cencora had obtained either directly from GlaxoSmithKline, or on behalf of GlaxoSmithKline, or from some other source.

168. In the letter, Cencora disclosed that the following Private Information of Plaintiff may have been disclosed during the Data Breach: name, address, date of birth, health diagnosis and/or medications and prescriptions. The letter identified that Plaintiff's Private Information was in Lash Group's possession through patient support and access programs that it manages on behalf of GlaxoSmithKline.

169. Cencora obtained or received, and continues to store and maintain, Plaintiff Angulo's Private Information. Cencora owed and owes Plaintiff Angulo a legal duty and obligation to protect his Private Information from unauthorized access and disclosure. Plaintiff Angulo's Private Information was compromised and disclosed as a result of Cencora's inadequate data security practices, which resulted in the Data Breach.

170. Plaintiff Angulo is very careful with his Private Information. Plaintiff Angulo either stores documents containing Private Information in a safe and secure location, or destroys the documents. Plaintiff Angulo would not have entrusted his Private Information to GlaxoSmithKline and/or Cencora, or otherwise would not have permitted his Private Information to be provided to GlaxoSmithKline and Cencora, had he known that Cencora maintains lax data security practices and is susceptible to data disclosures and privacy violations.

171. In response to the Data Breach, Plaintiff Angulo diligently undertook measures to mitigate its effects. This included purchasing LifeLock and Norton identity theft/credit monitoring services; placing a credit freeze with all three bureaus; researching the Data Breach; monitoring accounts for suspicious activity; changing account passwords; and requesting replacements for payment cards. He has invested considerable time addressing the fallout of the breach – time that would have otherwise been allocated to work or leisure activities. Regrettably, the time is irretrievably lost and cannot be reclaimed.

172. Plaintiff Angulo has also experienced attempted fraud since the occurrence of the Data Breach, including attempted fraudulent charges on Plaintiff Angulo's credit card; notifications from Lifelock that his information has been used to create new accounts and was found on the dark web; and a significant increase in suspicious spam calls, texts, and emails.

173. Plaintiff Angulo has suffered tangible harm resulting from the compromise of his Private Information due to the Data Breach, including, but not limited to: (i) an invasion of privacy; (ii) the unlawful appropriation of Private Information; (iii) a reduction or loss in the value of Private Information; (iv) expended time and opportunity costs incurred in mitigating the actual repercussions of the Data Breach; (v) statutory damages; (vi) nominal damages; and (vii) the

enduring and potentially escalating exposure of his Private Information to risk of unauthorized access and misuse by third parties.

174. The Data Breach has caused Plaintiff Angulo to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendants have still not fully informed him of key details about the Data Breach's occurrence.

175. As a result of the Data Breach, Plaintiff Angulo anticipates spending time and resources in the future to try to mitigate and address harms caused by the Data Breach.

176. As a result of the Data Breach, Plaintiff Angulo is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

177. Plaintiff Angulo has a continuing interest in ensuring that his Private Information, which remains in Defendants' possession, is protected and safeguarded from future breaches.

Plaintiff Sandra Weyerman

178. Plaintiff Sandra Weyerman is an individual who resides in Heflin, Alabama.

179. Plaintiff Weyerman participated in a patient support program and/or otherwise received healthcare, pharmaceuticals, or pharmaceutical related services from GlaxoSmithKline, which engaged Cencora and Lash Group to assist in providing those healthcare or pharmaceutical related services, including by collecting Weyerman's information on GlaxoSmithKline's behalf.

180. As a condition of participating in the patient support program and/or otherwise receiving healthcare or pharmaceutical related services, Plaintiff Weyerman provided Private Information either to GlaxoSmithKline directly, Cencora directly at the request of GlaxoSmithKline, or to her healthcare providers or pharmacies which provided that information to GlaxoSmithKline and/or Cencora indirectly.

181. Plaintiff Weyerman's health, treatment, healthcare provider, prescriptions, and other information related to her health care is highly private, and Plaintiff values that privacy. The release of that private information risks not only identity theft and/or fraud, among other similar harms, but also related harms such as the embarrassment, harassment, and discrimination that can result from release of private healthcare information.

182. Plaintiff Weyerman has a private medical condition for which she seeks medical care and the treatment of which requires one or more pharmaceutical drugs, which is highly private information. The privacy of Plaintiff Weyerman's health, treatment, healthcare provider, prescriptions, and other information related to her health care is important to Plaintiff Weyerman. The release of that information risks not only identity theft and/or fraud, among other similar harms, but also related harms such as the embarrassment, harassment, and discrimination that can result from release of private healthcare information.

183. Plaintiff Weyerman received a letter from Cencora dated May 24, 2024, notifying her that the Data Breach had impacted her Private Information, which Cencora had obtained either directly from GlaxoSmithKline, or on behalf of GlaxoSmithKline, or from some other source.

184. In the letter, Cencora disclosed that the following Private Information of Plaintiff may have been disclosed during the Data Breach: name, address, date of birth, health diagnosis and/or medications and prescriptions. The letter identified that Plaintiff's Private Information was in Lash Group's possession through patient support and access programs that it manages on behalf of GlaxoSmithKline.

185. Cencora obtained or received, and continues to store and maintain, Plaintiff Weyerman's Private Information. Cencora owed and owes Plaintiff Weyerman a legal duty and obligation to protect her Private Information from unauthorized access and disclosure. Plaintiff

Weyerman's Private Information was compromised and disclosed as a result of Cencora's inadequate data security practices, which resulted in the Data Breach.

186. Plaintiff Weyerman is very careful with her Private Information. Plaintiff Weyerman either stores documents containing Private Information in a safe and secure location, or destroys the documents. Plaintiff Weyerman would not have entrusted her Private Information to GlaxoSmithKline and/or Cencora, or otherwise would not have permitted her Private Information to be provided to GlaxoSmithKline and Cencora, had she known that Cencora maintains lax data security practices and is susceptible to data disclosures and privacy violations.

187. In response to the Data Breach, Plaintiff Weyerman diligently undertook measures to mitigate its effects. This included obtaining a credit freeze; researching the Data Breach; monitoring her accounts for suspicious activity; and changing her account passwords. She has invested considerable time addressing the fallout of the breach – time that would have otherwise been allocated to work or leisure activities. Regrettably, the time is irretrievably lost and cannot be reclaimed.

188. Plaintiff Weyerman has also experienced attempted fraud since the occurrence of the Data Breach, including an attempted fraudulent charge on her credit card; an increase in suspicious spam calls; and fraudulent attempts at opening a credit account.

189. Plaintiff Weyerman has suffered tangible harm resulting from the compromise of her Private Information due to the Data Breach, including, but not limited to: (i) an invasion of privacy; (ii) the unlawful appropriation of Private Information; (iii) a reduction or loss in the value of Private Information; (iv) expended time and opportunity costs incurred in mitigating the actual repercussions of the Data Breach; (v) statutory damages; (vi) nominal damages; and (vii) the

enduring and potentially escalating exposure of her Private Information to risk of unauthorized access and misuse by third parties.

190. The Data Breach has caused Plaintiff Weyerman to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendants have still not fully informed her of key details about the Data Breach's occurrence.

191. As a result of the Data Breach, Plaintiff Weyerman anticipates spending time and resources in the future to try to mitigate and address harms caused by the Data Breach.

192. As a result of the Data Breach, Plaintiff Weyerman is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

193. Plaintiff Weyerman has a continuing interest in ensuring that her Private Information, which remains in Defendants' possession, is protected and safeguarded from future breaches.

Plaintiff Peyton McQuillen

194. Plaintiff Peyton McQuillen is an individual who resides in Boca Raton, Florida.

195. Plaintiff McQuillen's health, treatment, healthcare provider, prescriptions, and other information related to his health care is highly private, and Plaintiff values that privacy. The release of that private information risks not only identity theft and/or fraud, among other similar harms, but also related harms such as the embarrassment, harassment, and discrimination that can result from release of private healthcare information.

196. Plaintiff McQuillen received a letter from Cencora dated May 20, 2024, notifying him that the Data Breach had impacted his Private Information, which Cencora had obtained through "one . . . organization in connection with its patient support programs."

197. In the letter, Cencora disclosed that the following Private Information of Plaintiff may have been disclosed during the Data Breach: name, address, date of birth, health diagnosis, and/or medications and prescriptions. The letter identified that Plaintiff's Private Information was in Lash Group's possession through patient support and access programs that it manages on behalf of "one . . . organization in connection with its patient support programs."

198. Cencora obtained or received, and continues to store and maintain, Plaintiff McQuillen's Private Information. Cencora owed and owes Plaintiff McQuillen a legal duty and obligation to protect his Private Information from unauthorized access and disclosure. Plaintiff McQuillen's Private Information was compromised and disclosed as a result of Cencora's inadequate data security practices, which resulted in the Data Breach.

199. Plaintiff McQuillen is very careful with his Private Information. Plaintiff McQuillen either stores documents containing Private Information in a safe and secure location, or destroys the documents. Plaintiff McQuillen would not have entrusted his Private Information to Cencora, or otherwise would not have permitted his Private Information to be provided to Cencora, had he known that Cencora maintains lax data security practices and is susceptible to data disclosures and privacy violations.

200. In response to the Data Breach, Plaintiff McQuillen diligently undertook measures to mitigate its effects, including researching the Data Breach; monitoring his accounts for suspicious activity; and purchasing a program to help decrease the amount of suspicious spam calls he received. He has invested considerable time addressing the fallout of the breach – time that would have otherwise been allocated to work or leisure activities. Regrettably, the time is irretrievably lost and cannot be reclaimed.

201. Plaintiff McQuillen has also experienced attempted fraud since the occurrence of the Data Breach, including experiencing such a significant increase in suspicious spam calls that he purchased a program to assist with blocking these attempts.

202. Plaintiff McQuillen has suffered tangible harm resulting from the compromise of his Private Information due to the Data Breach, including, but not limited to: (i) an invasion of privacy; (ii) the unlawful appropriation of Private Information; (iii) a reduction or loss in the value of Private Information; (iv) expended time and lost opportunity costs incurred in mitigating the actual repercussions of the Data Breach; (v) statutory damages; (vi) nominal damages; and (vii) the enduring and potentially escalating exposure of his Private Information to risk of unauthorized access and misuse by third parties.

203. The Data Breach has caused Plaintiff McQuillen to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendants have still not fully informed him of key details about the Data Breach's occurrence.

204. As a result of the Data Breach, Plaintiff McQuillen anticipates spending time and resources in the future to try to mitigate and address harms caused by the Data Breach.

205. As a result of the Data Breach, Plaintiff McQuillen is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

206. Plaintiff McQuillen has a continuing interest in ensuring that his Private Information, which remains in Defendants' possession, is protected and safeguarded from future breaches.

Plaintiff Mark Harrell

207. Plaintiff Mark Harrell is an individual who resides in Orlando, Florida.

208. Plaintiff Harrell participated in a patient support program and/or otherwise

received healthcare, pharmaceuticals, or pharmaceutical related services from BMS, which engaged Cencora and Lash Group to assist in providing healthcare or pharmaceutical related services, including by collecting Plaintiff Harrell's information on behalf of BMS.

209. As a condition of participating in the patient support program and/or otherwise receiving healthcare or pharmaceutical related services, Plaintiff Harrell provided Private Information either to BMS directly, Cencora directly at the request of BMS, or to his healthcare providers or pharmacies, which provided that information to BMS and/or Cencora indirectly.

210. Plaintiff Harrell's health, treatment, healthcare provider, prescriptions, and other information related to his health care is highly private and Plaintiff Harrell values that privacy. The release of that information risks not only identity theft and/or fraud, among other similar harms, but also related harms such as the embarrassment, harassment, and discrimination that can result from release of private healthcare information.

211. Plaintiff Harrell received a letter from Defendants dated May 17, 2024, notifying him that the Data Breach had impacted his Private Information, which Cencora had obtained either directly from BMS or on behalf of BMS, or from some other source.

212. In the letter, Cencora disclosed that the following Private Information of Plaintiff Harrell may have been disclosed during the Data Breach: first name, last name, address, date of birth, health diagnosis, and/or medications and prescriptions. The letter identified that Plaintiff Harrell's Private Information was in Lash Group's possession through patient support and access programs that it manages on behalf of BMS.

213. Cencora obtained or received and continues to store and maintain Plaintiff Harrell's Private Information. Cencora owed and owes Plaintiff Harrell a legal duty and obligation to protect his Private Information from unauthorized access and disclosure. Plaintiff Harrell's

Private Information was compromised and disclosed as a result of Cencora's inadequate data security practices, which resulted in the Data Breach.

214. Plaintiff Harrell is very careful with his Private Information. Plaintiff Harrell either stores documents containing Private Information in a safe and secure location, or destroys the documents. Plaintiff Harrell would not have entrusted his Private Information to BMS and/or Cencora, or otherwise would not have permitted his Private Information to be provided to BMS and/or Cencora, had he known that Cencora maintains lax data security practices and is susceptible to data disclosures and privacy violations.

215. In response to the Data Breach, Plaintiff Harrell diligently undertook measures to mitigate its effects. This included placing a freeze on his credit, changing his account passwords, researching the data breach, and spending a considerable amount of time monitoring his accounts for suspicious activity. He has invested considerable time addressing the fallout of the breach – time that would have otherwise been allocated to work or leisure activities. Regrettably, the time is irretrievably lost and cannot be reclaimed.

216. Plaintiff Harrell has also experienced attempted fraud since the occurrence of the Data Breach, including fraudulent inquiries on his credit report, notifications of changes to his credit score, and an increase in suspicious and unauthorized spam calls, texts, and emails.

217. Plaintiff Harrell has suffered tangible harm resulting from the compromise of his Private Information due to the Data Breach, including, but not limited to: (i) an invasion of privacy; (ii) the unlawful appropriation of Private Information; (iii) a reduction or loss in the value of Private Information; (iv) expended time and lost opportunity costs incurred in mitigating the actual repercussions of the Data Breach; (v) statutory damages; (vi) nominal damages; and (vii)

the enduring and potentially escalating exposure of his Private Information to risk of unauthorized access and misuse by third parties.

218. The Data Breach has caused Plaintiff Harrell to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendants have still not fully informed him of key details about the Data Breach's occurrence.

219. As a result of the Data Breach, Plaintiff Harrell anticipates spending time and resources in the future to try to mitigate and address harms caused by the Data Breach.

220. As a result of the Data Breach, Plaintiff Harrell is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

221. Plaintiff Harrell has a continuing interest in ensuring that his Private Information, which remains in Defendants' possession, is protected and safeguarded from future breaches.

Plaintiff Michelle Pettiford

222. Plaintiff Michelle Pettiford is an individual who resides in Frankfort, Ohio.

223. Plaintiff Pettiford participated in a patient support program and/or otherwise received healthcare, pharmaceuticals, or pharmaceutical related services from BMS, which engaged Cencora and Lash Group to assist in providing healthcare or pharmaceutical related services, including by collecting Plaintiff Pettiford's information on behalf of BMS.

224. As a condition of participating in the patient support program and/or otherwise receiving healthcare or pharmaceutical related services, Plaintiff Pettiford provided Private Information either to BMS directly, Cencora directly at the request of BMS, or to her healthcare providers or pharmacies, which provided that information to BMS and/or Cencora indirectly.

225. Plaintiff Pettiford's health, treatment, healthcare provider, prescriptions, and other information related to her health care is highly private, and Plaintiff Pettiford values that privacy.

The release of that information risks not only identity theft and/or fraud, among other similar harms, but also related harms such as the embarrassment, harassment, and discrimination that can result from release of private healthcare information.

226. Plaintiff Pettiford received a letter from Defendants dated May 17, 2024, notifying her that the Data Breach had impacted her Private Information, which Cencora had obtained either directly from BMS or on behalf of BMS, or from some other source.

227. In the letter, Cencora disclosed that the following Private Information of Plaintiff Pettiford may have been disclosed during the Data Breach: first name, last name, address, date of birth, health diagnosis, and/or medications and prescriptions. The letter identified that Plaintiff Pettiford's Private Information was in Lash Group's possession through patient support and access programs that it manages on behalf of BMS.

228. Cencora obtained or received and continues to store and maintain Plaintiff Pettiford's Private Information. Cencora owed and owes Plaintiff Pettiford a legal duty and obligation to protect her Private Information from unauthorized access and disclosure. Plaintiff Pettiford's Private Information was compromised and disclosed as a result of Cencora's inadequate data security practices, which resulted in the Data Breach.

229. Plaintiff Pettiford is very careful with her Private Information. Plaintiff Pettiford either stores documents containing Private Information in a safe and secure location, or destroys the documents. Plaintiff Pettiford would not have entrusted her Private Information to BMS and/or Cencora, or otherwise would not have permitted her Private Information to be provided to BMS and/or Cencora, had she known that Cencora maintains lax data security practices and is susceptible to data disclosures and privacy violations.

230. In response to the Data Breach, Plaintiff Pettiford diligently undertook measures

to mitigate its effects. This included monitoring her accounts for suspicious activity and changing her account passwords. She has invested considerable time addressing the fallout of the breach – time that would have otherwise been allocated to work or leisure activities. Regrettably, the time is irretrievably lost and cannot be reclaimed.

231. Plaintiff Pettiford has also experienced attempted fraud since the occurrence of the Data Breach, including an increase in suspicious and unauthorized spam calls, texts, and emails.

232. Plaintiff Pettiford has suffered tangible harm resulting from the compromise of her Private Information due to the Data Breach, including, but not limited to: (i) an invasion of privacy; (ii) the unlawful appropriation of Private Information; (iii) a reduction or loss in the value of Private Information; (iv) expended time and lost opportunity costs incurred in mitigating the actual repercussions of the Data Breach; (v) statutory damages; (vi) nominal damages; and (vii) the enduring and potentially escalating exposure of her Private Information to risk of unauthorized access and misuse by third parties.

233. The Data Breach has caused Plaintiff Pettiford to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendants have still not fully informed her of key details about the Data Breach's occurrence.

234. As a result of the Data Breach, Plaintiff Pettiford anticipates spending time and resources in the future to try to mitigate and address harms caused by the Data Breach.

235. As a result of the Data Breach, Plaintiff Pettiford is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

236. Plaintiff Pettiford has a continuing interest in ensuring that her Private Information, which remains in Defendants' possession, is protected and safeguarded from future breaches.

Plaintiff Bonnie Collins-White

237. Plaintiff Bonnie Collins-White is an individual who resides in Airville, Pennsylvania.

238. Plaintiff Collins-White health, treatment, healthcare provider, prescriptions, and other information related to her health care is highly private, and Plaintiff Collins-White values that privacy. The release of that private information risks not only identity theft and/or fraud, among other similar harms, but also related harms such as the embarrassment, harassment, and discrimination that can result from release of private healthcare information

239. Plaintiff Collins-White received a letter from Cencora dated May 28, 2024, notifying her that the Data Breach had impacted her Private Information, which Cencora had obtained through "one . . . organization in connection with its patient support programs."

240. In the letter, Defendants disclosed that the following Private Information of Plaintiff Collins-White may have been disclosed during the Data Breach: first name, last name, address, date of birth, health diagnosis, and/or medications and prescriptions. The letter identified that Plaintiff Collins-White's Private Information was in Lash Group's possession through patient support and access programs that it manages on behalf of "one . . . organization in connection with its patient support programs."

241. Cencora obtained or received and continues to store and maintain Plaintiff Collins-White's Private Information. Cencora owed and owes Plaintiff Collins-White a legal duty and obligation to protect her Private Information from unauthorized access and disclosure. Plaintiff Collins-White's Private Information was compromised and disclosed as a result of Cencora's inadequate data security practices, which resulted in the Data Breach.

242. Plaintiff Collins-White is very careful with her Private Information. Plaintiff

Collins-White either stores documents containing Private Information in a safe and secure location, or destroys the documents. Plaintiff Collins-White would not have entrusted her Private Information to Cencora, or otherwise would not have permitted her Private Information to be provided to Cencora, had she known that Cencora maintains lax data security practices and is susceptible to data disclosures and privacy violations.

243. In response to the Data Breach, Plaintiff Collins-White diligently undertook measures to mitigate its effects. This included signing up for a credit monitoring service, monitoring her accounts for suspicious activities, changing her account passwords, researching the data breach, and ordering a new debit card. She has invested considerable time addressing the fallout of the breach – time that would have otherwise been allocated to work or leisure activities. Regrettably, the time is irretrievably lost and cannot be reclaimed.

244. Plaintiff Collins-White has also experienced actual fraud since the occurrence of the Data Breach, including a drop in her credit score that prevented her from securing a lower interest rate on her mortgage and a significant increase in suspicious and unauthorized spam class, texts, and emails. Plaintiff Collins-White also was informed by her bank of fraudulent charges on her debit card, leading to its cancellation and reissuance.

245. Plaintiff Collins-White has suffered tangible harm resulting from the compromise of her Private Information due to the Data Breach, including, but not limited to: (i) an invasion of privacy; (ii) the unlawful appropriation of Private Information; (iii) a reduction or loss in the value of Private Information; (iv) expended time and lost opportunity costs incurred in mitigating the actual repercussions of the Data Breach; (v) statutory damages; (vi) nominal damages; and (vii) the enduring and potentially escalating exposure of her Private Information to risk of unauthorized access and misuse by third parties.

246. The Data Breach has caused Plaintiff Collins-White to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendants have still not fully informed her of key details about the Data Breach's occurrence.

247. As a result of the Data Breach, Plaintiff Collins-White anticipates spending time and resources in the future to try to mitigate and address harms caused by the Data Breach.

248. As a result of the Data Breach, Plaintiff Collins-White is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

249. Plaintiff Collins-White has a continuing interest in ensuring that her Private Information, which remains in Defendants' possession, is protected and safeguarded from future breaches.

Plaintiff James Soward

250. Plaintiff James Soward is an individual who resides in Tucson, Arizona.

251. Plaintiff Soward received a letter from Defendants dated May 16, 2024, notifying him that the Data Breach had impacted his Private Information, which Cencora had obtained through "one . . . organization in connection with its patient support programs."

252. In the letter, Cencora disclosed that the following Private Information of Plaintiff Soward may have been disclosed during the Data Breach: first name, last name, address, date of birth, health diagnosis, and/or medications and prescriptions. The letter identified that Plaintiff Soward's Private Information was in Lash Group's possession through patient support and access programs that it manages on behalf of "one . . . organization in connection with its patient support programs."

253. Plaintiff Soward's health, treatment, healthcare provider, prescriptions, and other information related to his health care is highly private, and Plaintiff Soward values that privacy.

The release of that private information risks not only identity theft and/or fraud, among other similar harms, but also related harms such as the embarrassment, harassment, and discrimination that can result from release of private healthcare information.

254. Cencora obtained or received and continues to store and maintain Plaintiff Soward's Private Information. Cencora owed and owes Plaintiff Soward a legal duty and obligation to protect his Private Information from unauthorized access and disclosure. Plaintiff Soward's Private Information was compromised and disclosed as a result of Cencora's inadequate data security practices, which resulted in the Data Breach.

255. Plaintiff Soward is very careful with his Private Information. Plaintiff Soward either stores documents containing Private Information in a safe and secure location, or destroys the documents. Plaintiff Soward would not have entrusted his Private Information to Cencora, or otherwise would not have permitted his Private Information to be provided to Cencora, had he known that Cencora maintains lax data security practices and is susceptible to data disclosures and privacy violations.

256. In response to the Data Breach, Plaintiff Soward diligently undertook measures to mitigate its effects. This included spending time monitoring his accounts for suspicious activity, changing account passwords, researching the data breach, and requesting that his payment cards be replaced. He has invested considerable time addressing the fallout of the breach – time that would have otherwise been allocated to work or leisure activities. Regrettably, the time is irretrievably lost and cannot be reclaimed.

257. Plaintiff Soward has suffered tangible harm resulting from the compromise of his Private Information due to the Data Breach, including, but not limited to: (i) an invasion of privacy; (ii) the unlawful appropriation of Private Information; (iii) a reduction or loss in the value

of Private Information; (iv) expended time and lost opportunity costs incurred in mitigating the actual repercussions of the Data Breach; (v) statutory damages; (vi) nominal damages; and (vii) the enduring and potentially escalating exposure of his Private Information to risk of unauthorized access and misuse by third parties.

258. The Data Breach has caused Plaintiff James to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendants have still not fully informed him of key details about the Data Breach's occurrence.

259. As a result of the Data Breach, Plaintiff Soward anticipates spending time and resources in the future to try to mitigate and address harms caused by the Data Breach.

260. As a result of the Data Breach, Plaintiff Soward is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

261. Plaintiff Soward has a continuing interest in ensuring that his Private Information, which remains in Defendants' possession, is protected and safeguarded from future breaches.

Plaintiff Katelyn Skowronski

262. Plaintiff Katelyn Skowronski is an individual who resides in Doylestown, Pennsylvania.

263. Plaintiff Skowronski's health, treatment, healthcare provider, prescriptions, and other information related to his/her health care is highly private, and Plaintiff Skowronski values that privacy. The release of that private information risks not only identity theft and/or fraud, among other similar harms, but also related harms such as the embarrassment, harassment, and discrimination that can result from release of private healthcare information.

264. Plaintiff Skowronski received a letter from Defendants dated May 28, 2024, notifying her that the Data Breach had impacted her Private Information, which Cencora had

obtained through "one . . . organization in connection with its patient support programs."

265. In the letter, Cencora disclosed that the following Private Information of Plaintiff Skowronski may have been disclosed during the Data Breach: first name, last name, address, date of birth, health diagnosis, and/or medications and prescriptions. The letter identified that Plaintiff Skowronski's Private Information was in Lash Group's possession through patient support and access programs that it manages on behalf of "one . . . organization in connection with its patient support programs."

266. Cencora obtained or received and continues to store and maintain Plaintiff Skowronski's Private Information. Cencora owed and owes Plaintiff Skowronski a legal duty and obligation to protect her Private Information from unauthorized access and disclosure. Plaintiff Skowronski's Private Information was compromised and disclosed as a result of Cencora's inadequate data security practices, which resulted in the Data Breach.

267. Plaintiff Skowronski is very careful with her Private Information. Plaintiff Skowronski either stores documents containing Private Information in a safe and secure location, or destroys the documents. Plaintiff Skowronski would not have entrusted her Private Information to Cencora, or otherwise would not have permitted her Private Information to be provided to Cencora, had she known that Cencora maintains lax data security practices and is susceptible to data disclosures and privacy violations.

268. In response to the Data Breach, Plaintiff Skowronski diligently undertook measures to mitigate its effects. This included monitoring her accounts for suspicious activity and changing her account passwords. She has invested considerable time addressing the fallout of the breach – time that would have otherwise been allocated to work or leisure activities. Regrettably, the time is irretrievably lost and cannot be reclaimed.

269. Plaintiff Skowronski has also experienced attempted fraud since the occurrence of the Data Breach, including an increase in suspicious and unauthorized spam calls and texts.

270. Plaintiff Skowronski has suffered tangible harm resulting from the compromise of her Private Information due to the Data Breach, including, but not limited to: (i) an invasion of privacy; (ii) the unlawful appropriation of Private Information; (iii) a reduction or loss in the value of Private Information; (iv) expended time and lost opportunity costs incurred in mitigating the actual repercussions of the Data Breach; (v) statutory damages; (vi) nominal damages; and (vii) the enduring and potentially escalating exposure of her Private Information to risk of unauthorized access and misuse by third parties.

271. The Data Breach has caused Plaintiff Skowronski to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendants have still not fully informed her of key details about the Data Breach's occurrence.

272. As a result of the Data Breach, Plaintiff Skowronski anticipates spending time and resources in the future to try to mitigate and address harms caused by the Data Breach.

273. As a result of the Data Breach, Plaintiff Skowronski is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

274. Plaintiff Skowronski has a continuing interest in ensuring that her Private Information, which remains in Defendants' possession, is protected and safeguarded from future breaches.

Plaintiff Robert Moskowitz

275. Plaintiff Robert Moskowitz is an individual who resides in Altoona, Pennsylvania.

276. Plaintiff Moskowitz participated in a patient support program and/or otherwise received healthcare, pharmaceuticals, or pharmaceutical related services from GlaxoSmithKline,

which engaged Cencora and Lash Group to assist in providing those healthcare or pharmaceutical related services, including by collecting Plaintiff Moskowitz's information on behalf of GlaxoSmithKline.

277. As a condition of participating in the patient support program and/or otherwise receiving healthcare or pharmaceutical related services, Plaintiff Moskowitz provided Private Information either to GlaxoSmithKline directly, Cencora directly at the request of GlaxoSmithKline, or to his healthcare providers or pharmacies, which provided that information to GlaxoSmithKline and/or Cencora indirectly.

278. Plaintiff Moskowitz's health, treatment, healthcare provider, prescriptions, and other information related to his health care is highly private, and Plaintiff Moskowitz values that privacy. The release of that information risks not only identity theft and/or fraud, among other similar harms, but also related harms such as the embarrassment, harassment, and discrimination that can result from release of private healthcare information.

279. Plaintiff Moskowitz received a letter from Defendants dated May 24, 2024, notifying him that the Data Breach had impacted his Private Information, which Cencora obtained either directly from GlaxoSmithKline or on behalf of GlaxoSmithKline, or from some other source.

280. In the letter, Cencora disclosed that the following Private Information of Plaintiff Moskowitz may have been disclosed during the Data Breach: first name, last name, address, date of birth, health diagnosis, and/or medications and prescriptions. The letter identified that Plaintiff Moskowitz's Private Information was in Lash Group's possession through patient support and access programs that it manages on behalf of GlaxoSmithKline.

281. Cencora obtained or received and continues to store and maintain Plaintiff

Moskowitz's Private Information. Cencora owed and owes Plaintiff Moskowitz a legal duty and obligation to protect his Private Information from unauthorized access and disclosure. Plaintiff Moskowitz's Private Information was compromised and disclosed as a result of Cencora's inadequate data security practices, which resulted in the Data Breach.

282. Plaintiff Moskowitz is very careful with his Private Information. Plaintiff Moskowitz either stores documents containing Private Information in a safe and secure location, or destroys the documents. Plaintiff Moskowitz would not have entrusted his Private Information to GlaxoSmithKline and/or Cencora, or otherwise would not have permitted his Private Information to be provided to GlaxoSmithKline and/or Cencora, had he known that Cencora maintains lax data security practices and is susceptible to data disclosures and privacy violations.

283. In response to the Data Breach, Plaintiff Moskowitz diligently undertook measures to mitigate its effects. This included monitoring his accounts for suspicious activity, changing his account passwords, disputing fraudulent charges, requesting that his payment cards be replaced, researching the data breach, and dealing with increased spam. He has invested considerable time addressing the fallout of the breach – time that would have otherwise been allocated to work or leisure activities. Regrettably, the time is irretrievably lost and cannot be reclaimed.

284. Plaintiff Moskowitz has also experienced actual fraud since the occurrence of the Data Breach, including fraudulent charges to his debit and credit cards (one of which his bank could not reverse) and an increase in suspicious and unauthorized spam calls, texts, and emails.

285. Plaintiff Moskowitz has suffered tangible harm resulting from the compromise of his Private Information due to the Data Breach, including, but not limited to: (i) an invasion of privacy; (ii) the unlawful appropriation of Private Information; (iii) a reduction or loss in the value of Private Information; (iv) expended time and opportunity costs incurred in mitigating the actual

repercussions of the Data Breach; (v) statutory damages; (vi) nominal damages; and (vii) the enduring and potentially escalating exposure of his Private Information to risk of unauthorized access and misuse by third parties.

286. The Data Breach has caused Plaintiff Moskowitz to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendants have still not fully informed him of key details about the Data Breach's occurrence.

287. As a result of the Data Breach, Plaintiff Moskowitz anticipates spending time and resources in the future to try to mitigate and address harms caused by the Data Breach.

288. As a result of the Data Breach, Plaintiff Moskowitz is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

289. Plaintiff Moskowitz has a continuing interest in ensuring that his Private Information, which remains in Defendants' possession, is protected and safeguarded from future breaches.

Plaintiff Ivery Johnson

290. Plaintiff Ivery Johnson is an individual who resides in Ridgeville, Ohio.

291. Plaintiff Johnson participated in a patient support program and/or otherwise received healthcare, pharmaceuticals, or pharmaceutical related services from BMS, which engaged Cencora and Lash Group to assist in providing that healthcare or pharmaceutical related services, including by collecting Plaintiff Johnson's information on behalf of BMS.

292. As a condition of participating in the patient support program and/or otherwise receiving healthcare or pharmaceutical related services, Plaintiff Johnson provided Private Information either to BMS directly, Cencora directly at the request of BMS, or to his healthcare providers or pharmacies, which provided that information to BMS and/or Cencora indirectly.

293. Plaintiff Johnson's health, treatment, healthcare provider, prescriptions, and other information related to his health care is highly private, and Plaintiff Johnson values that privacy. The release of that information risks not only identity theft and/or fraud, among other similar harms, but also related harms such as the embarrassment, harassment, and discrimination that can result from release of private healthcare information.

294. Plaintiff Johnson received a letter from Defendants dated May 17, 2024, notifying him that the Data Breach had impacted his Private Information, which Cencora had obtained either directly from BMS or on behalf of BMS, or from some other source.

295. In the letter, Cencora disclosed that the following Private Information of Plaintiff Johnson may have been disclosed during the Data Breach: first name, last name, address, date of birth, health diagnosis, and/or medications and prescriptions. The letter identified that Plaintiff Johnson's Private Information was in Lash Group's possession through patient support and access programs that it manages on behalf of BMS.

296. Cencora obtained or received and continues to store and maintain Plaintiff Johnson's Private Information. Cencora owed and owes Plaintiff Johnson a legal duty and obligation to protect his Private Information from unauthorized access and disclosure. Plaintiff Johnson's Private Information was compromised and disclosed as a result of Cencora's inadequate data security practices, which resulted in the Data Breach.

297. Plaintiff Johnson is very careful with his Private Information. Plaintiff Johnson either stores documents containing Private Information in a safe and secure location, or destroys the documents. Plaintiff Johnson would not have entrusted his Private Information to BMS and/or Cencora, or otherwise would not have permitted his Private Information to be provided to BMS

and/or Cencora, had he known that Cencora maintains lax data security practices and is susceptible to data disclosures and privacy violations.

298. In response to the Data Breach, Plaintiff Johnson diligently undertook measures to mitigate its effects. This included monitoring his accounts for suspicious activity. He has invested considerable time addressing the fallout of the breach – time that would have otherwise been allocated to work or leisure activities. Regrettably, the time is irretrievably lost and cannot be reclaimed.

299. Plaintiff Johnson has also experienced attempted fraud since the occurrence of the Data Breach, including a significant increase in suspicious and spam texts, calls, and emails.

300. Plaintiff Johnson has suffered tangible harm resulting from the compromise of his Private Information due to the Data Breach, including, but not limited to: (i) an invasion of privacy; (ii) the unlawful appropriation of Private Information; (iii) a reduction or loss in the value of Private Information; (iv) expended time and lost opportunity costs incurred in mitigating the actual repercussions of the Data Breach; (v) statutory damages; (vi) nominal damages; and (vii) the enduring and potentially escalating exposure of his Private Information to risk of unauthorized access and misuse by third parties.

301. The Data Breach has caused Plaintiff Johnson to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendants have still not fully informed him of key details about the Data Breach's occurrence.

302. As a result of the Data Breach, Plaintiff Johnson anticipates spending time and resources in the future to try to mitigate and address harms caused by the Data Breach.

303. As a result of the Data Breach, Plaintiff Johnson is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

304. Plaintiff Johnson has a continuing interest in ensuring that his Private Information, which remains in Defendants' possession, is protected and safeguarded from future breaches.

Plaintiff Theodore Tsangarinos

305. Plaintiff Theodore Tsangarinos is an individual who resides in Tarpon Springs, Florida.

306. Plaintiff Tsangarinos participated in a patient support program and/or otherwise received healthcare, pharmaceuticals, or pharmaceutical related services from BMS and Novartis, which engaged Cencora and Lash Group to assist in providing that healthcare or pharmaceutical related services, including by collecting Plaintiff Tsangarinos' information on behalf of BMS and Novartis.

307. As a condition of participating in the patient support program and/or otherwise receiving healthcare or pharmaceutical related services, Plaintiff Tsangarinos provided Private Information either to BMS and/or Novartis directly, Cencora directly at the request of BMS and/or Novartis, or to his healthcare providers or pharmacies, which provided that information to BMS, Novartis, and/or Cencora indirectly.

308. Plaintiff Tsangarinos' health, treatment, healthcare provider, prescriptions, and other information related to his health care is highly private, and Plaintiff Tsangarinos values that privacy. The release of that private information risks not only identity theft and/or fraud, among other similar harms, but also related harms such as the embarrassment, harassment, and discrimination that can result from release of private healthcare information.

309. Plaintiff Tsangarinos received a letter from Defendants dated May 18, 2024, notifying him that the Data Breach had impacted his Private Information, which Cencora had obtained either directly from BMS or on behalf of BMS, or from some other source. In the letter,

Cencora disclosed that the following Private Information of Plaintiff Tsangarinos may have been disclosed during the Data Breach: first name, last name, address, date of birth, health diagnosis, and/or medications and prescriptions. The letter identified that Plaintiff Tsangarinos' Private Information was in Lash Group's possession through patient support and access programs that it manages on behalf of BMS.

310. Plaintiff Tsangarinos received a second letter from Cencora dated May 22, 2024, notifying him that the Data Breach had impacted his Private Information, which Cencora had obtained either directly from Novartis or on behalf of Novartis, or from some other source. In the letter, Cencora disclosed that the following Private Information of Plaintiff Tsangarinos may have been disclosed during the Data Breach: first name, last name, address, date of birth, health diagnosis, and/or medications and prescriptions. The letter identified that Plaintiff Tsangarinos' Private Information was in Lash Group's possession through patient support and access programs that it manages on behalf of Novartis.

311. Cencora obtained or received and continues to store and maintain Plaintiff Tsangarinos' Private Information. Cencora owed and owes Plaintiff Tsangarinos a legal duty and obligation to protect his Private Information from unauthorized access and disclosure. Plaintiff Tsangarinos' Private Information was compromised and disclosed as a result of Cencora's inadequate data security practices, which resulted in the Data Breach.

312. Plaintiff Tsangarinos is very careful with his Private Information. Plaintiff Tsangarinos either stores documents containing Private Information in a safe and secure location, or destroys the documents. Plaintiff Tsangarinos would not have entrusted his Private Information to BMS, Novartis, and/or Cencora, or otherwise would not have permitted his Private Information

to be provided to BMS, Novartis, and/or Cencora, had he known that Cencora maintains lax data security practices and is susceptible to data disclosures and privacy violations.

313. In response to the Data Breach, Plaintiff Tsangarinos diligently undertook measures to mitigate its effects. This included monitoring his accounts for suspicious activity, changing his account passwords, researching the data breach, and replacing his payment cards. He has invested considerable time addressing the fallout of the breach – time that would have otherwise been allocated to work or leisure activities. Regrettably, the time is irretrievably lost and cannot be reclaimed.

314. Plaintiff Tsangarinos has also experienced attempted fraud since the occurrence of the Data Breach, including decreases in his credit score and an increase in suspicious and unauthorized spam calls, texts, and emails.

315. Plaintiff Tsangarinos has suffered tangible harm resulting from the compromise of his Private Information due to the Data Breach, including, but not limited to: (i) an invasion of privacy; (ii) the unlawful appropriation of Private Information; (iii) a reduction or loss in the value of Private Information; (iv) expended time and opportunity costs incurred in mitigating the actual repercussions of the Data Breach; (v) statutory damages; (vi) nominal damages; and (vii) the enduring and potentially escalating exposure of his Private Information to risk of unauthorized access and misuse by third parties.

316. The Data Breach has caused Plaintiff Tsangarinos to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendants have still not fully informed him of key details about the Data Breach's occurrence.

317. As a result of the Data Breach, Plaintiff Tsangarinos anticipates spending time and resources in the future to try to mitigate and address harms caused by the Data Breach.

318. As a result of the Data Breach, Plaintiff Tsangarinos is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

319. Plaintiff Tsangarinos has a continuing interest in ensuring that his Private Information, which remains in Defendants' possession, is protected and safeguarded from future breaches.

Plaintiff Tuan Nguyen

320. Plaintiff Tuan Nguyen is an individual who resides in Fountain Valley, California.

321. Plaintiff Nguyen participated in a patient support program and/or otherwise received healthcare, pharmaceuticals, or pharmaceutical related services from Pfizer, which engaged Cencora and Lash Group to assist in providing that healthcare or pharmaceutical related services, including by collecting Plaintiff Nguyen's information on behalf of Pfizer.

322. As a condition of participating in the patient support program and/or otherwise receiving healthcare or pharmaceutical related services, Plaintiff Nguyen provided Private Information either to Pfizer directly, Cencora directly at the request of Pfizer, or to his healthcare providers or pharmacies, which provided that information to Pfizer and/or Cencora indirectly.

323. Plaintiff Nguyen's health, treatment, healthcare provider, prescriptions, and other information related to his health care is highly private, and Plaintiff Nguyen values that privacy. The release of that information risks not only identity theft and/or fraud, among other similar harms, but also related harms such as the embarrassment, harassment, and discrimination that can result from release of private healthcare information.

324. Plaintiff Nguyen received a letter from Defendants dated June 7, 2024, notifying him that the Data Breach had impacted his Private Information, which Cencora had obtained either directly from Pfizer or on behalf of Pfizer, or from some other source.

325. In the letter, Defendants disclosed that the following Private Information of Plaintiff Nguyen may have been disclosed during the Data Breach: first name, last name, address, date of birth, health diagnosis, and/or medications and prescriptions. The letter identified that Plaintiff Nguyen's Private Information was in Lash Group's possession through patient support and access programs that it manages on behalf of Pfizer.

326. Cencora obtained or received and continues to store and maintain Plaintiff Nguyen's Private Information. Cencora owed and owes Plaintiff Nguyen a legal duty and obligation to protect his Private Information from unauthorized access and disclosure. Plaintiff Nguyen's Private Information was compromised and disclosed as a result of Cencora's inadequate data security practices, which resulted in the Data Breach.

327. Plaintiff Nguyen is very careful with his Private Information. Plaintiff Nguyen either stores documents containing Private Information in a safe and secure location, or destroys the documents. Plaintiff Nguyen would not have entrusted his Private Information to Pfizer and/or Cencora, or otherwise would not have permitted his Private Information to be provided to Pfizer and Cencora, had he known that Cencora maintains lax data security practices and is susceptible to data disclosures and privacy violations.

328. In response to the Data Breach, Plaintiff Nguyen diligently undertook measures to mitigate its effects. This included placing a freeze on his credit, monitoring his accounts for suspicious activity, changing his account passwords, and replacing his payment cards. He has invested considerable time addressing the fallout of the breach—time that would have otherwise been allocated to work or leisure activities. Regrettably, the time is irretrievably lost and cannot be reclaimed.

329. Plaintiff Nguyen has also experienced actual fraud since the occurrence of the Data

Breach, including fraudulent charges on his credit card, attempts to obtain government benefits in his name, and an increase in spam and suspicious calls, texts and emails.

330. Plaintiff Nguyen has suffered tangible harm resulting from the compromise of his Private Information due to the Data Breach, including, but not limited to: (i) an invasion of privacy; (ii) the unlawful appropriation of Private Information; (iii) a reduction or loss in the value of Private Information; (iv) expended time and opportunity costs incurred in mitigating the actual repercussions of the Data Breach; (v) statutory damages; (vi) nominal damages; and (vii) the enduring and potentially escalating exposure of his Private Information to risk of unauthorized access and misuse by third parties.

331. The Data Breach has caused Plaintiff Nguyen to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendants have still not fully informed him of key details about the Data Breach's occurrence.

332. As a result of the Data Breach, Plaintiff Nguyen anticipates spending time and resources in the future to try to mitigate and address harms caused by the Data Breach.

333. As a result of the Data Breach, Plaintiff Nguyen is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

334. Plaintiff Nguyen has a continuing interest in ensuring that his Private Information, which remains in Defendants' possession, is protected and safeguarded from future breaches.

Plaintiff Debra Brown

335. Plaintiff Debra Brown is an individual who resides in Oyster Bay, New York.

336. Plaintiff Brown's health, treatment, healthcare provider, prescriptions, and other information related to her health care is highly private, and Plaintiff Brown values that privacy. The release of that private information risks not only identity theft and/or fraud, among other

similar harms, but also related harms such as the embarrassment, harassment, and discrimination that can result from release of private healthcare information.

337. Plaintiff Brown received a letter from Defendants dated May 30, 2024, notifying her that the Data Breach had impacted her Private Information, which Cencora had obtained through "one . . . organization in connection with its patient support programs."

338. In the letter, Cencora disclosed that the following Private Information of Plaintiff Brown may have been disclosed during the Data Breach: first name, last name, address, date of birth, health diagnosis, and/or medications and prescriptions. The letter identified that Plaintiff Brown's Private Information was in Lash Group's possession through patient support and access programs that it manages on behalf of "one . . . organization in connection with its patient support programs."

339. Cencora obtained or received and continues to store and maintain Plaintiff Brown's Private Information. Cencora owed and owes Plaintiff Brown a legal duty and obligation to protect her Private Information from unauthorized access and disclosure. Plaintiff Brown's Private Information was compromised and disclosed as a result of Cencora's inadequate data security practices, which resulted in the Data Breach.

340. Plaintiff Brown is very careful with her Private Information. Plaintiff Brown either stores documents containing Private Information in a safe and secure location, or destroys the documents. Plaintiff Brown would not have entrusted her Private Information to Cencora, or otherwise would not have permitted her Private Information to be provided to Cencora, had she known that Cencora maintains lax data security practices and is susceptible to data disclosures and privacy violations.

341. In response to the Data Breach, Plaintiff Brown diligently undertook measures to mitigate its effects. This included monitoring her accounts for suspicious activity, researching the data breach, and changing her account passwords. She has invested considerable time addressing the fallout of the breach – time that would have otherwise been allocated to work or leisure activities. Regrettably, the time is irretrievably lost and cannot be reclaimed.

342. Plaintiff Brown has also experienced attempted fraud since the occurrence of the Data Breach, including a significant increase in suspicious and spam texts, calls, and emails.

343. Plaintiff Brown has suffered tangible harm resulting from the compromise of her Private Information due to the Data Breach, including, but not limited to: (i) an invasion of privacy; (ii) the unlawful appropriation of Private Information; (iii) a reduction or loss in the value of Private Information; (iv) expended time and opportunity costs incurred in mitigating the actual repercussions of the Data Breach; (v) statutory damages; (vi) nominal damages; and (vii) the enduring and potentially escalating exposure of her Private Information to risk of unauthorized access and misuse by third parties.

344. The Data Breach has caused Plaintiff Brown to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendants have still not fully informed her of key details about the Data Breach's occurrence.

345. As a result of the Data Breach, Plaintiff Brown anticipates spending time and resources in the future to try to mitigate and address harms caused by the Data Breach.

346. As a result of the Data Breach, Plaintiff Brown is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

347. Plaintiff Brown has a continuing interest in ensuring that her Private Information, which remains in Defendants' possession, is protected and safeguarded from future breaches.

Plaintiff Lisa DeSmet

348. Plaintiff Lisa DeSmet is an individual who resides in Brookings, South Dakota.

349. Plaintiff DeSmet's health, treatment, healthcare provider, prescriptions, and other information related to her health care is highly private, and Plaintiff DeSmet values that privacy. The release of that private information risks not only identity theft and/or fraud, among other similar harms, but also related harms such as the embarrassment, harassment, and discrimination that can result from release of private healthcare information.

350. Plaintiff DeSmet received a letter from Defendants dated May 21, 2024, notifying her that the Data Breach had impacted her Private Information, which Cencora had obtained through "one . . . organization in connection with its patient support programs."

351. In the letter, Cencora disclosed that the following Private Information of Plaintiff DeSmet may have been disclosed during the Data Breach: first name, last name, address, date of birth, health diagnosis, and/or medications and prescriptions. The letter identified that Plaintiff DeSmet's Private Information was in Lash Group's possession through patient support and access programs that it manages on behalf of "one . . . organization in connection with its patient support programs."

352. Cencora obtained or received and continues to store and maintain Plaintiff DeSmet's Private Information. Cencora owed and owes Plaintiff DeSmet a legal duty and obligation to protect her Private Information from unauthorized access and disclosure. Plaintiff DeSmet's Private Information was compromised and disclosed as a result of Cencora's inadequate data security practices, which resulted in the Data Breach.

353. Plaintiff DeSmet is very careful with her Private Information. Plaintiff DeSmet either stores documents containing Private Information in a safe and secure location, or destroys

the documents. Plaintiff DeSmet would not have entrusted her Private Information to Cencora, or otherwise would not have permitted her Private Information to be provided to Cencora, had she known that Cencora maintains lax data security practices and is susceptible to data disclosures and privacy violations.

354. In response to the Data Breach, Plaintiff DeSmet diligently undertook measures to mitigate its effects. This included placing a freeze on her credit, monitoring her accounts for suspicious activity, changing her account passwords, researching the data breach, and replacing her payment cards. She has invested considerable time addressing the fallout of the breach – time that would have otherwise been allocated to work or leisure activities. Regrettably, the time is irretrievably lost and cannot be reclaimed.

355. Plaintiff DeSmet has suffered tangible harm resulting from the compromise of her Private Information due to the Data Breach, including, but not limited to: (i) an invasion of privacy; (ii) the unlawful appropriation of Private Information; (iii) a reduction or loss in the value of Private Information; (iv) expended time and opportunity costs incurred in mitigating the actual repercussions of the Data Breach; (v) statutory damages; (vi) nominal damages; and (vii) the enduring and potentially escalating exposure of her Private Information to risk of unauthorized access and misuse by third parties.

356. The Data Breach has caused Plaintiff DeSmet to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendants have still not fully informed her of key details about the Data Breach's occurrence.

357. As a result of the Data Breach, Plaintiff DeSmet anticipates spending time and resources in the future to try to mitigate and address harms caused by the Data Breach.

358. As a result of the Data Breach, Plaintiff DeSmet is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

359. Plaintiff DeSmet has a continuing interest in ensuring that her Private Information, which remains in Defendants' possession, is protected and safeguarded from future breaches.

Plaintiff Bridget Reardon

360. Plaintiff Bridget Reardon is an individual who resides in Long Island City, New York.

361. Plaintiff Reardon's health, treatment, healthcare provider, prescriptions, and other information related to her health care is highly private, and Plaintiff Reardon values that privacy. The release of that private information risks not only identity theft and/or fraud, among other similar harms, but also related harms such as the embarrassment, harassment, and discrimination that can result from release of private healthcare information.

362. Plaintiff Reardon received a letter from Defendants dated May 28, 2024, notifying her that the Data Breach had impacted her Private Information, which Cencora had obtained through "one . . . organization in connection with its patient support programs."

363. In the letter, Cencora disclosed that the following Private Information of Plaintiff Reardon may have been disclosed during the Data Breach: first name, last name, address, date of birth, health diagnosis, and/or medications and prescriptions. The letter identified that Plaintiff Reardon's Private Information was in Lash Group's possession through patient support and access programs that it manages on behalf of "one . . . organization in connection with its patient support programs."

364. Cencora obtained or received and continues to store and maintain Plaintiff Reardon's Private Information. Cencora owed and owes Plaintiff Reardon a legal duty and

obligation to protect her Private Information from unauthorized access and disclosure. Plaintiff Reardon's Private Information was compromised and disclosed as a result of Cencora's inadequate data security practices, which resulted in the Data Breach.

365. Plaintiff Reardon is very careful with her Private Information. Plaintiff Reardon either stores documents containing Private Information in a safe and secure location, or destroys the documents. Plaintiff Reardon would not have entrusted her Private Information to Cencora, or otherwise would not have permitted her Private Information to be provided to Cencora, had she known that Cencora maintains lax data security practices and is susceptible to data disclosures and privacy violations.

366. In response to the Data Breach, Plaintiff Reardon diligently undertook measures to mitigate its effects. This included placing a freeze on her credit, monitoring her accounts for suspicious activity, changing her account passwords, and replacing her payment cards. She has invested considerable time addressing the fallout of the breach – time that would have otherwise been allocated to work or leisure activities. Regrettably, the time is irretrievably lost and cannot be reclaimed.

367. Plaintiff Reardon has also experienced attempted fraud since the occurrence of the Data Breach, including an increase in suspicious and unauthorized spam texts, calls, and emails and a drop in her credit score.

368. Plaintiff Reardon has suffered tangible harm resulting from the compromise of her Private Information due to the Data Breach, including, but not limited to: (i) an invasion of privacy; (ii) the unlawful appropriation of Private Information; (iii) a reduction or loss in the value of Private Information; (iv) expended time and lost opportunity costs incurred in mitigating the actual repercussions of the Data Breach; (v) statutory damages; (vi) nominal damages; and (vii)

the enduring and potentially escalating exposure of her Private Information to risk of unauthorized access and misuse by third parties.

369. The Data Breach has caused Plaintiff Reardon to suffer fear, anxiety, and stress, which has been compounded by the fact that Cencora has still not fully informed her of key details about the Data Breach's occurrence.

370. As a result of the Data Breach, Plaintiff Reardon anticipates spending time and resources in the future to try to mitigate and address harms caused by the Data Breach.

371. As a result of the Data Breach, Plaintiff Reardon is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

372. Plaintiff Bridget has a continuing interest in ensuring that her Private Information, which remains in Defendants' possession, is protected and safeguarded from future breaches.

Plaintiff Michael Williamson

373. Plaintiff Michael Williamson is an individual who resides in Lake Ozark, Missouri.

374. Plaintiff Williamson's health, treatment, healthcare provider, prescriptions, and other information related to his health care is highly private, and Plaintiff Williamson values that privacy. The release of that private information risks not only identity theft and/or fraud, among other similar harms, but also related harms such as the embarrassment, harassment, and discrimination that can result from release of private healthcare information.

375. Plaintiff Williamson received a letter from Defendants dated May 23, 2024, notifying him that the Data Breach had impacted his Private Information, which Cencora had obtained through "one . . . organization in connection with its patient support programs."

376. In the letter, Defendants disclosed that the following Private Information of Plaintiff Williamson may have been disclosed during the Data Breach: first name, last name, address, date of birth, health diagnosis, and/or medications and prescriptions. The letter identified that Plaintiff Williamson's Private Information was in Lash Group's possession through patient support and access programs that it manages on behalf of "one . . . organization in connection with its patient support programs."

377. Cencora obtained or received and continues to store and maintain Plaintiff Williamson's Private Information. Cencora owed and owes Plaintiff Williamson a legal duty and obligation to protect his Private Information from unauthorized access and disclosure. Plaintiff Williamson's Private Information was compromised and disclosed as a result of Cencora's inadequate data security practices, which resulted in the Data Breach.

378. Plaintiff Williamson is very careful with his Private Information. Plaintiff Williamson either stores documents containing Private Information in a safe and secure location, or destroys the documents. Plaintiff Williamson would not have entrusted his Private Information to Cencora, or otherwise would not have permitted his Private Information to be provided to Cencora, had he known that Cencora maintains lax data security practices and is susceptible to data disclosures and privacy violations.

379. In response to the Data Breach, Plaintiff Williamson diligently undertook measures to mitigate its effects. This included monitoring his accounts for suspicious activity and researching the data breach. He has invested considerable time addressing the fallout of the breach – time that would have otherwise been allocated to work or leisure activities. Regrettably, the time is irretrievably lost and cannot be reclaimed.

380. Plaintiff Williamson has also experienced attempted fraud since the occurrence of the Data Breach, including an increase in suspicious and unauthorized spam texts, calls, and emails.

381. Plaintiff Williamson has suffered tangible harm resulting from the compromise of his Private Information due to the Data Breach, including, but not limited to: (i) an invasion of privacy; (ii) the unlawful appropriation of Private Information; (iii) a reduction or loss in the value of Private Information; (iv) expended time and opportunity costs incurred in mitigating the actual repercussions of the Data Breach; (v) statutory damages; (vi) nominal damages; and (vii) the enduring and potentially escalating exposure of his Private Information to risk of unauthorized access and misuse by third parties.

382. The Data Breach has caused Plaintiff Williamson to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendants have still not fully informed him of key details about the Data Breach's occurrence.

383. As a result of the Data Breach, Plaintiff Williamson anticipates spending time and resources in the future to try to mitigate and address harms caused by the Data Breach.

384. As a result of the Data Breach, Plaintiff Williamson is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

385. Plaintiff Williamson has a continuing interest in ensuring that his Private Information, which remains in Defendants' possession, is protected and safeguarded from future breaches.

Plaintiff Amanda Tucker

386. Plaintiff Amanda Tucker is an individual who resides in Oakland, California.

387. Plaintiff Tucker's health, treatment, healthcare provider, prescriptions, and other

information related to her health care is highly private, and Plaintiff Tucker values that privacy. The release of that private information risks not only identity theft and/or fraud, among other similar harms, but also related harms such as the embarrassment, harassment, and discrimination that can result from release of private healthcare information.

388. Plaintiff Tucker received a letter from Defendants dated May 28, 2024, notifying her that the Data Breach had impacted her Private Information, which Cencora had obtained through "one . . . organization in connection with its patient support programs."

389. In the letter, Cencora disclosed that the following Private Information of Plaintiff Tucker may have been disclosed during the Data Breach: first name, last name, address, date of birth, health diagnosis, and/or medications and prescriptions. The letter identified that Plaintiff Tucker's Private Information was in Lash Group's possession through patient support and access programs that it manages on behalf of "one . . . organization in connection with its patient support programs."

390. Cencora obtained or received and continues to store and maintain Plaintiff Tucker's Private Information. Cencora owed and owes Plaintiff Tucker a legal duty and obligation to protect her Private Information from unauthorized access and disclosure. Plaintiff Tucker's Private Information was compromised and disclosed as a result of Cencora's inadequate data security practices, which resulted in the Data Breach.

391. Plaintiff Tucker is very careful with her Private Information. Plaintiff Tucker, including not liberally sharing her Private Information, using incognito mode on the internet, and either storing documents containing Private Information in a safe and secure location, or destroying the documents. Plaintiff Tucker would not have entrusted her Private Information to Cencora, or otherwise would not have permitted her Private Information to be provided to

Cencora, had she known that Cencora maintains lax data security practices and is susceptible to data disclosures and privacy violations.

392. In response to the Data Breach, Plaintiff Tucker diligently undertook measures to mitigate its effects. This included placing a freeze on her credit, monitoring her accounts, paying out-of-pocket for credit monitoring, and changing her account passwords. She has invested considerable time and expenses addressing the fallout of the breach – time and money that would have otherwise been allocated to work or leisure activities. Regrettably, the time is irretrievably lost and cannot be reclaimed.

393. Plaintiff Tucker has also experienced attempted fraud since the occurrence of the Data Breach, including an increase in suspicious and unauthorized spam texts, calls, and emails.

394. Plaintiff Tucker has suffered tangible harm resulting from the compromise of her Private Information due to the Data Breach, including, but not limited to: (i) an invasion of privacy; (ii) the unlawful appropriation of Private Information; (iii) a reduction or loss in the value of Private Information; (iv) expended time and opportunity costs incurred in mitigating the actual repercussions of the Data Breach; (v) statutory damages; (vi) nominal damages; and (vii) the enduring and potentially escalating exposure of her Private Information to risk of unauthorized access and misuse by third parties.

395. The Data Breach has caused Plaintiff Tucker to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendants have still not fully informed her of key details about the Data Breach's occurrence.

396. As a result of the Data Breach, Plaintiff Tucker anticipates spending time and resources in the future to try to mitigate and address harms caused by the Data Breach.

397. As a result of the Data Breach, Plaintiff Tucker is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

398. Plaintiff Tucker has a continuing interest in ensuring that her Private Information, which remains in Defendants' possession, is protected and safeguarded from future breaches.

Plaintiff Margie Lopez

399. Plaintiff Margie Lopez is an individual who resides in La Quinta, California.

400. Plaintiff Lopez participated in a patient support program and/or otherwise received healthcare, pharmaceuticals, or pharmaceutical related services from BMS, which engaged Cencora and Lash Group to assist in providing that healthcare or pharmaceutical related services, including by collecting Plaintiff Lopez's information on behalf of BMS.

401. As a condition of participating in the patient support program and/or otherwise receiving healthcare or pharmaceutical related services, Plaintiff Lopez provided Private Information either to BMS directly, Cencora directly at the request of BMS, or to her healthcare providers or pharmacies, which provided that information to BMS and/or Cencora indirectly.

402. Plaintiff Lopez's health, treatment, healthcare provider, prescriptions, and other information related to her health care is highly private, and Plaintiff Lopez values that privacy. The release of that information risks not only identity theft and/or fraud, among other similar harms, but also related harms such as the embarrassment, harassment, and discrimination that can result from release of private healthcare information.

403. Plaintiff Lopez received a letter from Defendants dated May 17, 2024, notifying her that the Data Breach had impacted her Private Information, which Cencora had obtained either directly from BMS or on behalf of BMS, or from some other source.

404. In the letter, Defendants disclosed that the following Private Information of

Plaintiff Lopez may have been disclosed during the Data Breach: first name, last name, address, date of birth, health diagnosis, and/or medications and prescriptions. The letter identified that Plaintiff Lopez's Private Information was in Lash Group's possession through patient support and access programs that it manages on behalf of BMS.

405. Cencora obtained or received and continues to store and maintain Plaintiff Lopez's Private Information. Cencora owed and owes Plaintiff Lopez a legal duty and obligation to protect her Private Information from unauthorized access and disclosure. Plaintiff Lopez's Private Information was compromised and disclosed as a result of Cencora's inadequate data security practices, which resulted in the Data Breach.

406. Plaintiff Lopez is very careful with her Private Information. Plaintiff Lopez either stores documents containing Private Information in a safe and secure location, or destroys the documents. Plaintiff Lopez would not have entrusted her Private Information to BMS and/or Cencora, or otherwise would not have permitted her Private Information to be provided to BMS and Cencora, had she known that Cencora maintains lax data security practices and is susceptible to data disclosures and privacy violations.

407. In response to the Data Breach, Plaintiff Lopez diligently undertook measures to mitigate its effects. This included placing a freeze on her credit, monitoring her accounts for suspicious activity, changing her account passwords, researching the data breach and methods to protect her identity once Private Information is posted on the dark web, and replacing her payment cards. She has invested considerable time addressing the fallout of the breach – time that would have otherwise been allocated to work or leisure activities. Regrettably, the time is irretrievably lost and cannot be reclaimed.

408. Plaintiff Lopez has also experienced attempted fraud since the occurrence of the

Data Breach, including receiving notifications that her Private Information is available on the dark web, spam mail at an address she only provided to Defendants through their partner companies and suspicious spam calls, emails, and texts asking for personal information, and notification of a reduction in her credit score.

409. Plaintiff Lopez has suffered tangible harm resulting from the compromise of her Private Information due to the Data Breach, including, but not limited to: (i) an invasion of privacy; (ii) the unlawful appropriation of Private Information; (iii) a reduction or loss in the value of Private Information; (iv) expended time and opportunity costs incurred in mitigating the actual repercussions of the Data Breach; (v) statutory damages; (vi) nominal damages; and (vii) the enduring and potentially escalating exposure of her Private Information to risk of unauthorized access and misuse by third parties.

410. The Data Breach has caused Plaintiff Lopez to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendants have still not fully informed her of key details about the Data Breach's occurrence.

411. As a result of the Data Breach, Plaintiff Lopez anticipates spending time and resources in the future to try to mitigate and address harms caused by the Data Breach.

412. As a result of the Data Breach, Plaintiff Lopez is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

413. Plaintiff Lopez has a continuing interest in ensuring that her Private Information, which remains in Defendants' possession, is protected and safeguarded from future breaches.

Defendants

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

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

JURISDICTION AND VENUE

416. This Court has original jurisdiction under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2), because this is a class action involving more than 100 putative Class members and the amount in controversy exceeds $5,000,000, exclusive of interest and costs. And minimal diversity is established because Plaintiffs (and many members of the proposed Class) are citizens of states different from Defendants.

417. This Court has jurisdiction over Defendants because Defendants Cencora, Inc. and Lash Group operate their principal places of business within this District, indicating a deliberate engagement with the markets here, and operate and direct commerce within this District. Consequently, the exercise of jurisdiction by this Court is not only justified but also appropriate, given Defendants' intentional involvement in this District's economic activities.

418. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(b) because Defendants Cencora, Inc. and Lash Group maintain their principal places of business in this District and a substantial part of the events, acts, and omissions giving rise to Plaintiffs' claims occurred in this District.

FACTUAL ALLEGATIONS

Defendants' Business

419. Defendant Cencora, Inc.—formerly known as AmerisourceBergen[11]—is a leading pharmaceutical solutions organization that provides "end-to-end pharmaceutical commercialization solutions" and claims to "empower[] patient-centered care all over the world."[12] Cencora, Inc. "connects manufacturers, providers, pharmacies, and patients" to provide drug distribution and consulting services.[13]

420. Defendant Lash Group, a subsidiary of Cencora, Inc.,[14] "partners with pharmaceutical companies, pharmacies, and healthcare providers to facilitate access to therapies through drug distribution, patient support and services, business analytics and technology, and other services."[15]

421. In the regular course of their business, Defendants, on behalf of and under the name of the Drug Companies and other similar companies that Defendants provide

[11] *See AmerisourceBergen becomes Cencora, in alignment with the company's growing global footprint and central role in pharmaceutical access and care*, CENCORA (Aug. 30, 2023), https://www.cencora.com/newsroom/amerisourcebergen-becomes-cencora.
[12] *Who we are*, CENCORA, https://www.cencora.com/who-we-are (last visited Feb. 24, 2025).
[13] *Human Health*, CENCORA, https://www.cencora.com/human-health (last visited Feb. 24, 2025).
[14] The Lash Group, n.2, *supra*.
[15] *Notice of Data Security Incident*, LASH GROUP, https://web.archive.org/web/20240713222724/http://www.lashgroup.com:80/notice (last visited Feb. 24, 2025).

pharmaceutical-related services to, collected, stored, and processed the Private Information of Plaintiffs and Class members, either directly or indirectly requiring Plaintiffs and Class members to provide their Private Information as a condition of receiving pharmaceutical services, special prices for pharmaceuticals, or other benefits. In the regular course of their business, Defendants also collected, stored, and processed the Private Information of employees of and other individuals associated with Cencora divisions and/or affiliated companies.

422. For example, a patient, desiring to take advantage of a drug company's patient assistance programs (such as free or reduced price drugs or co-pay assistance), would go to the applicable website for a particular drug and would there be directed to either call a toll free phone number or submit their personal information (including in many cases their health and financial information) online or via fax or email (or all four methods). On information and belief, the information the individual provided would be transmitted to Defendants for purposes of determining eligibility for and administering the services offered by Defendants' drug company clients. Thereafter, Defendants would administer the Drug Companies' services, collecting and storing patient or consumer personal information.

423. The Data Breach resulted in the exfiltration of Private Information not only from healthcare-related databases but also included Private Information about employees and/or customers of one or more Cencora divisions and/or affiliated companies.

424. This Private Information was highly sensitive and, on information and belief, included some or all of the following:

a. Full names and addresses;

b. Dates of birth;

c. Social Security numbers;

d. Health insurance information, including policy and group numbers;

e. Health information, including diagnoses, prescriptions, personal medical and treatment histories, family medical histories, and mental health information;

f. Information about physicians and related medical professionals (including pharmacies) involved in prior or ongoing treatment of the individual;

g. Personal email addresses and phone numbers;

h. Driver's license (or other similar state identifications) information;

i. Account login information and passwords; and

j. Medicare/Medicaid information.

425. This sort of Private Information is extremely sensitive and is highly valuable to criminals because it can be used to commit identity theft and medical theft crimes.

426. Because of the highly sensitive and personal nature of the information about Plaintiffs and Class members that Defendants collect, process, and store, Defendants are obligated to, among other things: keep Private Information private; comply with data security standards applicable within the healthcare industry, including guidelines promulgated by the Federal Trade Commission ("FTC"); and comply with all applicable federal and state laws protecting consumer Private Information.

427. As business entities covered under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), Defendants also are required to implement and maintain adequate safeguards to prevent unauthorized use or disclosure of Private Information, including by implementing the requirements of the HIPAA Security Rule.

Defendants' Privacy Policies and Practices

428. Cencora, Inc.'s website states "Cencora, Inc. and its affiliate companies

('Cencora') value and protect the personal information entrusted to the company by its suppliers, customers, and visitors. As a United States company doing business around the world, Cencora maintains a comprehensive privacy program designed to comply with its legal obligations under applicable law."[16]

429. Lash Group's website contains a Notice of Privacy Practices (the "Privacy Policy") that tells customers and potential customers "how Lash Group may use and disclose your health information."[17] The Privacy Policy describes that it will use its customers' health information for treatment, payment, and healthcare operations, among others.[18]

430. Lash Group admits it is required by law to follow the Privacy Policy and further admits it is required by law to maintain the privacy of PHI.[19]

431. The Privacy Policy promises "Lash Group respects the confidentiality of your health information and will protect it in a responsible and professional manner."[20]

432. According to the Privacy Policy, Lash Group is required to "obtain your written authorization to use or disclose your health information for reasons other than those listed [in the Privacy Policy] and permitted under law."[21]

433. On information and belief, Defendants also had a duty to protect Plaintiffs' and Class Members' personal information as agents of the Drug Companies on whose behalf they operate and collect the personal information.

---

[16] *Privacy Statement Overview*, CENCORA, https://www.cencora.com/global-privacy-statement-overview (last visited Feb. 24. 2025).
[17] *Notice of Privacy Practices*, LASH GROUP (July 1, 2012), https://web.archive.org/web/20240730200533/https://www.lashgroup.com/notice-of-privacy-practices (last visited Feb. 24, 2025).
[18] *Id.*
[19] *Id.*
[20] *Id.*
[21] *Id.*

434. Despite what Defendants promise in their own policies, and despite the existence of their legal and equitable duties to protect Plaintiffs' and Class members' Private Information, Defendants did not maintain adequate security to protect their systems from infiltration by cyber criminals.

435. Plaintiffs and the Class members trusted these assurances and counted on these sophisticated business entities to maintain the confidentiality and security of their sensitive Private Information. They expected Defendants to use this information solely for business purposes and to make only authorized disclosures. Plaintiffs and Class members, in general, insist on security measures to protect their Private Information, particularly when it involves sensitive details like health-related information and SSNs.

The Data Breach

436. On February 27, 2024, Cencora filed a Form 8-K with the SEC disclosing that it had failed to prevent a data breach that resulted in the theft of sensitive personal information. The SEC filing confirmed that "[o]n February 21, 2024, Cencora learned that data from its information systems had been exfiltrated, some of which may contain personal information."[22] The filing omitted crucial information, including the date(s) on which the Data Breach actually occurred, how cybercriminals gained access to the encrypted files on its systems, what computer systems were impacted, the means and mechanisms of the cyberattack, how it determined that the Personal Information had been accessed, and of particular importance to Plaintiffs and Class members, what actual steps Cencora took following the Data Breach to secure its systems and train its employees to prevent further cyberattacks. To this day, these critical details have not been explained or clarified to Plaintiffs and Class members, who maintain a vested interest in

[22] *SEC Filing,* n.3, *supra*.

safeguarding their Private Information. Without such essential details, the ability of Plaintiffs and Class members to effectively mitigate the resulting harms is significantly limited.

437. In May of 2024, two months after discovering the Data Breach, Cencora began sending out letters to impacted individuals. The breach notice letters received by Plaintiffs indicate that the investigation into the Data Breach determined that personal information was impacted, including at least individuals' names, addresses, dates of birth, health diagnoses, and medication or prescription information.

438. On July 31, 2024, Cencora filed an amended Form 8-K Form with the SEC, disclosing that it had discovered additional data which was exfiltrated during the Data Breach. The amended filing confirmed that the Data Breach resulted in the exfiltration of more data than initially reported by Cencora, including PII and PHI.

439. At approximately the same time, Cencora also publicly announced the Data Breach on its website, stating:[23]

> The Lash Group partners with pharmaceutical companies, pharmacies, and healthcare providers to facilitate access to therapies through drug distribution, patient support and services, business analytics and technology, and other services. . . . Lash Group is providing substitute notice of an event that involved certain individuals' personal information and/or protected health information that Lash Group was in possession of through its current or past partnerships with organizations in connection with its patient support programs. . . . On February 21, 2024, Lash Group learned that data from its information systems had been exfiltrated, some of which could contain personal information. Upon initial detection of the unauthorized activity, we immediately took containment steps and commenced an investigation with the assistance of law enforcement, cybersecurity experts and outside lawyers. On May 8, 2024, Lash Group confirmed that individuals' personal information may have been involved in the incident.

440. Despite the intentional opacity from Cencora regarding the details of this incident, the SEC filings, subsequent breach notice letters sent to Plaintiffs, and the investigative reporting

[23] *Notice of Data Security Incident*, CENCORA, https://www.cencora.com/caredx-notice.

following the Data Breach provide several discernable facts: a) the Data Breach was perpetrated by well-known cybercriminals, specifically the Dark Angels; b) these cybercriminals initially breached Cencora's networks and systems before exfiltrating data; and c) within Cencora's networks and systems, the cybercriminals specifically targeted information—such as Plaintiffs' and Class members' PHI, PII, and other sensitive data—for download and theft.

441. The information compromised in the Data Breach included Plaintiffs' and Class members' PII and PHI, as defined by HIPAA.

442. As detailed further below, Defendants were bound by obligations stemming from the Federal Trade Commission Act ("FTC Act"), HIPAA, common law principles, industry standards, and other requirements to maintain the confidentiality of Plaintiffs' and Class members' Private Information and safeguard it against unauthorized access and disclosure.

443. Defendants failed to implement reasonable security procedures and practices commensurate with the sensitivity of the information they held concerning Plaintiffs and Class members. This lapse led to the exposure of Private Information, which could have been mitigated through reasonable and adequate information security controls.

444. The hackers successfully accessed and obtained unencrypted Private Information of Plaintiffs and Class members.

445. The Dark Angels group was financially motivated and intentionally targeted Plaintiffs' and Class members' highly valuable Private Information. The *modus operandi* of cybercriminals like the Dark Angels group is to distribute their targets' (here, Plaintiffs' and Class members') Private Information through illicit criminal networks, possibly including on the dark web.

Defendants Acquired, Collected, and Stored Plaintiffs' and Class Members' Private Information

446. Defendants acquire, collect, and store massive amounts of Private Information relating to Plaintiffs and Class members as a routine part of their business.

447. As a condition of receiving medications, financial assistance, and other healthcare or employment related services, Plaintiffs and Class members were required to entrust Cencora, directly or indirectly, with highly sensitive personal information.

448. By directly or indirectly collecting, processing, and storing Plaintiffs' and Class members' Private Information, Defendants each assumed legal and equitable duties to protect such information. Each Defendant knew or should have known that it was responsible for protecting this Private Information from disclosure.

449. Plaintiffs and Class members would not have entrusted their Private Information to Defendants absent a promise to safeguard this information from unauthorized disclosure.

450. Plaintiffs and Class members relied on Defendants to keep their Private Information confidential and securely maintained.

451. The injuries to Plaintiffs and Class members were directly and proximately caused by Defendants' failure to implement and maintain adequate data security measures for the Private Information of Plaintiffs and Class members.

452. The ramifications of Defendants' failure to properly secure the Private Information of Plaintiffs and Class members are long lasting and severe. Once Private Information is stolen, fraudulent use of that information and resulting damage to victims may continue for years.

453. As healthcare industry entities in custody of Plaintiffs' and Class members' Private Information, Defendants knew or should have known the importance of safeguarding the Private Information in their possession, custody, or control, and of the foreseeable consequences of their

data security systems being breached. This includes the significant costs imposed on Plaintiffs and Class members as a result of the Data Breach. Defendants failed, however, to take adequate cybersecurity measures to prevent the Data Breach.

Plaintiffs' Private Information Has Value

Private Information Has Significant Value to Criminals

454. Criminal actors highly value PHI and PII. Such information is continually traded on underground marketplaces, including on the dark web, a section of the internet that cannot be accessed through standard web browsers.

455. The FTC recommends that identity theft victims take several steps to protect their Personal Information after a data breach, including contacting one of the three credit bureaus to place a fraud alert (and to consider an extended fraud alert that lasts for seven years if identity theft occurs), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[24]

456. There may also be a substantial time lag—measured in years—between when harm occurs versus when it is discovered, and also between when Personal Information is stolen and when it is used. According to a report by the U.S. Government Accountability Office ("GAO"):

> [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

[24] *Identity Theft Recovery Steps*, FTC, https://www.identitytheft.gov/Steps (last visited Feb. 24, 2025). Indeed, the FTC takes data breaches seriously, and has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information can constitute an "unfair practice" in violation of the FTC Act. *See, e.g.*, *FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015).

> the harm resulting from data breaches cannot necessarily rule out all future harm.[25]

457. Personal Information is such an inherently valuable commodity to identity thieves that, once it is compromised, criminals often trade the information on the cyber black-market for years.

458. Private Information can be sold at a price ranging from $40 to $200 per individual.[26] Medical records are valued at up to $1,000 per individual depending on completeness.[27]

459. PII also sells on legitimate markets, an industry that is valued at hundreds of billions of dollars per year. Individuals can sell their own non-public information directly to data brokers who aggregate the information for sale to marketers or others.

Private Information Has Value for Its Owners, and That Value Is Diminished by Theft

460. Unauthorized disclosure of sensitive Private Information also reduces its value to its rightful owner, as recognized by courts as an independent source of harm.[28] PHI constitutes a valuable property right.[29]

---

[25] *Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, at 2, U.S. GOV'T ACCOUNTABILITY OFF. (June 4, 2007), https://www.gao.gov/assets/gao-07-737.pdf ("GAO Report").

[26] Brian Stack, *Here's How Much Your Personal Information Is Selling for on the Dark Web*, EXPERIAN (Dec. 6, 2017), https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/.

[27] *Id.*

[28] *See In re Marriott Int'l, Inc., Customer Data Sec. Breach Litig.*, 440 F. Supp. 3d 447, 462 (D. Md. 2020) ("Neither should the Court ignore what common sense compels it to acknowledge—the value that personal identifying information has in our increasingly digital economy. Many companies, like Marriott, collect personal information. Consumers too recognize the value of their personal information and offer it in exchange for goods and services.").

[29] *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 1 (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).

461. Even consumers who have been victims of previous data breaches are injured when their data is stolen and traded. Each data breach increases the likelihood that the victim's personal information will be exposed on the dark web or otherwise sold to those who are looking to misuse it.

462. The leak of the kind of information exposed in the Data Breach poses a significant risk to Plaintiffs and Class members. Unlike data breaches that involve credit card information, the information (such as health information and SSNs) taken in the Cencora data breach is immutable, and so Plaintiffs and Class members cannot easily protect themselves by changing it.

463. SSNs—which, according to available information, were almost certainly compromised in the Data Breach—are one of the most detrimental forms of Private Information to have stolen due to the multitude of fraudulent purposes for which they can be used and the significant challenge individuals face in changing them.

464. According to the Social Security Administration, each time an individual's SSN is compromised, "the potential for a thief to illegitimately gain access to bank accounts, credit cards, driving records, tax and employment histories and other private information increases."[30] Moreover, "[b]ecause many organizations still use SSNs as the primary identifier, exposure to identity theft and fraud remains."[31]

465. An individual cannot obtain a new SSN without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a SSN is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new SSN.

---

[30] *See Avoid Identity Theft: Protect Social Security Numbers,* SOC. SEC. PHILA. REG., https://www.ssa.gov/phila/ProtectingSSNs.htm (last visited Feb. 24, 2025).
[31] *Id.*

466. Even then, a new SSN may not be effective. According to Julie Ferguson of the Identity Theft Resource Center ("ITRC"), "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[32]

467. Identity theft presents many challenges. In a survey, the ITRC found that most victims of identity crimes need more than a month to resolve issues stemming from identity theft and some need over a year.[33]

468. There may be a time lag between when sensitive personal information is stolen, when it is used, and when a person discovers it has been used. On average, it takes approximately three months for a consumer to discover their identity has been stolen and used and it takes some individuals up to three years to learn that information.[34]

469. Theft of PHI, which was also compromised in the Data Breach, is also gravely serious, putting patients at risk of medical identity theft wherein "[a] thief may use your name or health insurance numbers to see a doctor, get prescription drugs, file claims with your insurance provider, or get other care. If the thief's health information is mixed with yours, your treatment, insurance and payment records, and credit report may be affected."[35]

470. Data breaches involving medical information "typically leave[] a trail of falsified

---

[32] Bryan Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015, 4:59 AM), http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millionsworrying-about-identity-theft.
[33] *ITRC Annual Data Breach Report 2023*, ITRC (2023), https://www.idtheftcenter.org/publication/2023-data-breach-report/.
[34] John W. Coffey, *Difficulties in Determining Data Breach Impacts*, 17 J. of Systemics, Cybernetics and Informatics 9 (2019), https://iiisci.org/journal/pdv/sci/pdfs/IP069LL19.pdf .
[35] *Medical I.D. Theft*, EFRAUDPREVENTION, https://efraudprevention.net/embed/cody/Medical_I.D._theft.html (last visited Feb. 24, 2025).

information in medical records that can plague victims' medical and financial lives for years."[36]

471. Medical identity theft "is also more difficult to detect, taking almost twice as long as normal identity theft."[37] In warning consumers of the dangers of medical identity theft, the FTC states that an identity thief may use Personal Information "to see a doctor, get prescription drugs, buy medical devices, submit claims with your insurance provider, or get other medical care."[38] The FTC also warns, "[i]f the thief's health information is mixed with yours, your treatment, insurance and payment records, and credit report may be affected."[39]

472. A report published by the World Privacy Forum[40] and presented at the U.S. FTC Workshop on Informational Injury describes what medical identity theft victims may experience:

a. Changes to their health care records, most often the addition of falsified information, through improper billing activity or activity by imposters. These changes can affect the healthcare a person receives if the errors are not caught and corrected.

b. Significant bills for medical goods and services not sought or received.

c. Issues with insurance, co-pays, and insurance caps.

d. Long-term credit problems based on problems with debt collectors reporting debt due to identity theft.

e. Serious life consequences resulting from the crime; for example, victims have been falsely accused of being drug users based on falsified entries to their medical files; victims have had their children removed from them due

[36] Patrick Lucas Austin, "*It Is Absurd." Data Breaches Show It's Time to Rethink How We Use Social Security Numbers, Experts Say*, TIME (Aug. 5, 2019, 3:39 PM), https://time.com/5643643/capital-one-equifax-data-breach-social-security/.
[37] Pam Dixon & John Emerson, *The Geography of Medical Identity Theft*, WORLD PRIVACY FORUM (Dec. 12, 2017), https://www.worldprivacyforum.org/wp-content/uploads/2017/12/WPF_Geography_of_Medical_Identity_Theft_fs.pdf.
[38] *See Health Care Systems and Medical Devices at Risk for Increased Cyber Intrusions for Financial Gain*, FBI (Apr. 8, 2014) at 14, https://publicintelligence.net/fbi-health-care-cyber-intrusions/.
[39] *See What to Know About Medical Identity Theft*, FTC, https://consumer.ftc.gov/articles/what-know-about-medical-identity-theft (last visited Nov. 26, 2024).
[40] *The Geography of Medical Identity Theft*, n.37, *supra*.

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

f. As a result of improper and/or fraudulent medical debt reporting, victims may not qualify for mortgages or other loans and may experience other financial impacts.

g. Phantom medical debt collection based on medical billing or other identity information.

h. Sales of medical debt arising from identity theft can perpetuate a victim's debt collection and credit problems, through no fault of their own.

473. A study conducted by Experian revealed that the average cost of medical identity theft for victims per incident is approximately $20,000. Additionally, the majority of victims of medical identity theft are compelled to cover out-of-pocket expenses for healthcare services they did not receive in order to reinstate their coverage. Furthermore, almost half of medical identity theft victims lose their healthcare coverage following the incident, while nearly one-third experience an increase in insurance premiums. Alarmingly, 40 percent of victims are unable to fully resolve their identity theft ordeal.[41]

474. Fraudulent medical treatment also has non-financial impacts. Deborah Peel, executive director of Patient Privacy Rights, has described scenarios in which an individual may be given an improper blood type or administered medicines because their medical records contain information supplied by an individual obtaining treatment under a false name.[42]

475. Further, loss of personal health information, such as treatment history, diagnoses,

[41] *The Truth Behind Medical Identity Theft: What You Don't Know Can Cost You*, EXPERIAN, (Mar. 3, 2010), https://www.experianplc.com/newsroom/press-releases/2010/the-truth-behind-medical-identity-theft-what-you-don-t-know-can-cost-you.

[42] *See* Andrea Peterson, *2015 is already the year of the health-care hack—and it's only going to get worse*, WASH. POST (Mar. 20, 2015), available at http://www.washingtonpost.com/blogs/the-switch/wp/2015/03/20/2015-is-already-the-year-of-the-health-care-hack-and-its-only-going-to-get-worse/.

and prescription information, exposes the victims to loss of reputation, loss of employment, blackmail, and other harms including the trauma of having their most personal details published online for all to see.

476. Even where victims receive reimbursement for resulting financial losses, they are not made whole again. The Identity Theft Resource Center's 2021 survey reported that victims of identity theft reported suffering the following negative experiences and emotional harms: anxiety (84%); feelings of violation (76%); rejection for credit or loans (83%); financial related identity problems (32%); resulting problems with family members (32%); and feeling suicidal (10%).[43]

477. Physical harms also result from identity theft. A similar survey found that victims suffered the following resulting physical symptoms: sleep disturbances (48.3%); inability to concentrate / lack of focus (37.1%); inability to work because of physical symptoms (28.7%); new physical illnesses including stomach problems, pain, and heart palpitations (23.1%); and starting or relapsing into unhealthy or addictive behaviors (12.6%).[44]

478. As a result, beyond financial harms, data breaches also have a deep, psychological impact on their victims.

> In some ways, a cyber attack can feel like the digital equivalent of getting robbed, with a corresponding wave of anxiety and dread. Anxiety, panic, fear, and frustration—even intense anger—are common emotional responses when experiencing a cyber attack. While expected, these emotions can paralyze you and prolong or worsen a cyber attack.[45]

---

[43] *2021 Consumer Aftermath Report: How Identity Crimes Impact Victims, their Families, Friends, and Workplaces*, at 6, IDENTITY THEFT RES. CTR. (2021), https://www.idtheftcenter.org/wp-content/uploads/2021/09/ITRC_2021_Consumer_Aftermath_Report.pdf.

[44] *Identity Theft: The Aftermath 2017*, IDENTITY THEFT RES. CTR., at 12, https://www.idtheftcenter.org/wp-content/uploads/images/page-docs/Aftermath_2017.pdf (last visited June 7, 2024).

[45] Amber Steel, *The Psychological Impact of Cyber Attacks*, LastPass (Aug. 17, 2022), https://blog.lastpass.com/posts/the-psychological-impact-of-cyber-attacks.

479. Plaintiffs and Class members place a significant value on data security. About half of consumers consider data security to be a main or important consideration in their purchasing decisions and would be willing to pay more to work with those with better data security. Likewise, 70% of consumers would provide less personal information to organizations that suffered a data breach.[46]

480. As a result, Plaintiffs and Class members must take significant protective measures, including years of constant surveillance of their financial and personal records, credit monitoring, and identity protection.

Defendants Should Have Foreseen and Prevented the Data Breach

481. At all relevant times, Defendants knew or should have known that their data systems would be targeted for attack by cybercriminals. Nothing about this attack was extraordinary. Cybercriminals commonly target the healthcare industry due to the troves of confidential health and personal information maintained and stored by healthcare organizations.

482. Cyberattacks against the healthcare industry in particular have been common for over a decade, with the FBI warning as early as 2011 that cybercriminals targeting healthcare providers and others were "advancing their abilities to attack a system remotely" and "[o]nce a system is compromised, cyber criminals will use their accesses to obtain PII."[47]

483. The FBI again warned healthcare stakeholders in 2014 that they are the target of hackers, stating "[t]he FBI has observed malicious actors targeting healthcare related systems,

[46] *Beyond the Bottom Line: The Real Cost of Data Breaches,* FIREEYE, p. 14, (May 2016), https://web.archive.org/web/20230628100935/https://www2.fireeye.com/rs/848-DID-242/images/rpt-beyond-bottomline.pdf.

[47] Gordon M. Snow, FBI, *Statement before the House Financial Services Committee, Subcommittee on Financial Institutions and Consumer Credit*, The FBI Testimony (Sept. 14, 2011), https://archives.fbi.gov/archives/news/testimony/cyber-security-threats-to-the-financial-sector.

perhaps for the purpose of obtaining Protected Healthcare Information (PHI) and/or Personally Identifiable Information (PII)."[48]

484. Additionally, in light of recent high profile cybersecurity incidents at other healthcare partner and provider companies, including HCA Healthcare (11 million patients, July 2023), Managed Care of North America (8 million patients, March 2023), PharMerica Corporation (5 million patients, March 2023), HealthEC LLC (4 million patients, July 2023), ESO Solutions, Inc. (2.7 million patients, September 2023), Prospect Medical Holdings, Inc. (1.3 million patients, July-August 2023), and American Medical Collection Agency (25 million patients, March 2019), Defendants knew or should have known that its electronic records would be targeted by cybercriminals.

485. According to an article in the HIPAA Journal posted on November 2, 2023, cybercriminals hack into healthcare networks for their "highly prized" medical records. "[T]he number of data breaches reported by HIPAA-regulated entities continues to increase every year. 2021 saw 714 data breaches of 500 or more records reported to the [HHS' Office for Civil Rights] OCR – an 11% increase from the previous year. Almost three-quarters of those breaches were classified as hacking/IT incidents."[49]

486. Under the HIPAA Privacy Rules, a breach is defined as, "[t]he acquisition, access, use, or disclosure of PHI in a manner not permitted under the [HIPAA Privacy Rule] which

[48] *See FBI Cyber Bulletin: Malicious Actors Targeting Protected Health Information*, FEDERAL BUREAU OF INVESTIGATION (Aug. 19, 2014), https://publicintelligence.net/fbi-targeting-healthcare/.
[49] Steve Alder, *Editorial: Why Do Criminals Target Medical Records*, THE HIPAA JOURNAL (Nov. 2, 2023), https://www.hipaajournal.com/why-do-criminals-target-medical-records.

compromises the security or privacy of the PHI."[50] Accordingly, an attack such as the one that was discovered on or about February 21, 2024 is considered a breach under the HIPAA Rules because there was an access of PHI not permitted under the HIPAA Privacy Rule.

487. Such an attack is also considered a "Security Incident" under HIPAA. Under the HIPAA Rules, a "Security Incident" is defined as "the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system." 45 CFR § 164.304. According to the U.S. Department of Health and Human Services, "[t]he presence of ransomware (or any malware) on a covered entity's or business associate's computer systems is a security incident under the HIPAA Security Rule."[51]

488. Data Breaches can be prevented. Cybersecurity professionals and applicable information security standards urge organizations to take reasonable technical and administrative information security controls. Commonly recommended controls include: ensuring computer networks are adequately segmented, implementing and configuring intrusion prevention and detection technologies, monitoring computer systems using appropriate tools and responding to alerts on suspicious behavior, implementing spam and malware filters, requiring multifactor authentication for access, implementing secure cryptographic algorithms, timely applying security patches and updates, limiting the use of privileged or administrative accounts, training employees on the handling of suspicious emails, implementing an effective vulnerability management program, ensuring vendors implement and maintain adequate security controls, and

[50] *See Fact Sheet: Ransomware and HIPAA*, U.S. DEP'T OF HEALTH & HUM. SERV'S, https://www.hhs.gov/hipaa/for-professionals/security/guidance/cybersecurity/ransomware-fact-sheet/index.html (last visited Feb. 24. 2025).
[51] *See id.*

implementing heightened security controls around sensitive data sources.

489. The Data Breach underscores Defendants' failure to sufficiently implement one or more vital security measures aimed at preventing cyberattacks. The Data Breach never would have occurred without Defendants' inadequate cybersecurity controls, enabling data thieves to access and acquire the Private Information of hundreds of thousands to millions of individuals, including Plaintiffs and Class members.

490. Defendants knew that unprotected or exposed Private Information in the custody of healthcare companies is valuable and highly sought after by nefarious third parties seeking to illegally monetize that Private Information through unauthorized access.

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

492. Plaintiffs and Class members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their Private Information.

Defendants Did Not Comply with Federal Law and Regulatory Guidance

Defendants Did Not Comply with FTC Guidelines

493. The United States government issues guidelines for businesses that store sensitive data to help them minimize the risks of a data breach. The FTC publishes guides for businesses

about the importance of reasonable data security practices.[52] In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which sets forth data security principles and practices for businesses to protect sensitive data.[53] The FTC tells businesses to (a) protect the personal information they collect and store; (b) dispose of personal information it no longer needs; (c) encrypt information on their networks; (d) understand their network's vulnerabilities; (e) put policies in place to correct security problems.

494. The FTC also recommends that healthcare 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.[54]

495. The FTC further recommends that healthcare businesses not maintain Personal 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.[55]

496. The FTC brings enforcement actions against businesses that fail to reasonably protect customer information. The Commission treats the failure to use reasonable care and appropriate measures to protect against unauthorized access to confidential customer data as an

[52] *Start with Security: A Guide for Business*, FED. TRADE COMM'N (Aug. 2023), https://www.ftc.gov/business-guidance/resources/start-security-guide-business (last visited Feb. 24, 2025).
[53] *Protecting Personal Information: A Guide for Business*, FED. TRADE COMM'N (Oct. 2016), https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business (last visited Feb. 24, 2025).
[54] *Id*.
[55] *Start with Security: A Guide for Business*, n.52, *supra*.

unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45. Orders issued in these actions state the measures required for businesses to meet their data security obligations.[56]

497. These FTC enforcement actions include actions against healthcare industry companies like Defendants. *See, e.g., In the Matter of LabMd, Inc., A Corp*, No. 9357, 2016 WL 4128215, at *32 (F.T.C. July 28, 2016)*, vacated on other grounds*, *LabMD, Inc. v. Fed. Trade Comm'n,* 894 F.3d 1221 (11th Cir. 2018) ("[T]he Commission concludes that LabMD's data security practices were unreasonable and constitute an unfair act or practice in violation of Section 5 of the FTC Act).

498. Defendants knew of their obligations to implement and use basic data security practices to protect to Plaintiffs' and Class members' Private Information properly.

499. Still, Defendants failed to comply with those recommendations and guidelines, which if followed would have prevented the Data Breach. This failure to reasonably protect against unauthorized access to Private Information is an unfair act or practice under Section 5 of the FTC Act, 15 U.S.C. § 45.

500. Defendants' failure to protect Plaintiffs' and Class members' Private Information suggests their failure to comply fully with standard cybersecurity practices such as those described above.

Defendants Did Not Comply with HIPAA Guidelines

501. Defendants provide healthcare, medication, pharmacy, and pharmaceutical related services to hundreds of millions of individuals annually either directly or via their healthcare

[56] *Privacy and Security Enforcement*, FED. TRADE COMM'N., https://www.ftc.gov/news-events/topics/protecting-consumer-privacy-security/privacy-security-enforcement (last visited Feb. 24, 2025).

clients. As a regular and necessary part of their businesses, Defendants directly or indirectly collect, store, and transfer the highly sensitive Private Information of individuals.

502. As covered entities, Defendants are required under federal and state law to maintain the strictest confidentiality of the Private Information they acquire, receive, collect, transfer, and store. Defendants are further required to maintain sufficient safeguards to protect that Private Information from being accessed by unauthorized third parties.

503. In fact, whenever Defendants contract with healthcare providers to provide various business and medical services, HIPAA requires that these contracts mandate that Defendants will use adequate safeguards to prevent unauthorized use or disclosure of PHI, including by implementing the HIPAA Security Rule[57] and immediately reporting any unauthorized use or disclosure of PHI such as the Data Breach.

504. For their part, Defendants Cencora and Lash Group explicitly tout their commitment to protecting the privacy of private information, claiming that:

> Cencora, Inc. and its affiliate companies ("Cencora") *value and protect the personal information* entrusted to the company by its suppliers, customers, and visitors. As a United States company doing business around the world, Cencora *maintains a comprehensive privacy program* designed to comply with its legal obligations under applicable law.[58]

505. The Data Breach resulted from a combination of multiple failures by the Defendants to adequately and reasonably secure the Plaintiffs' and Class members' Private Information in violation of the mandates set forth in HIPAA's regulations.

---

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

[58] *Privacy Statement Overview*, CENCORA, https://www.cencora.com/global-privacy-statement-overview (last visited Feb. 24, 2025) (emphasis added).

Defendants Did Not Comply with Industry Standards

506. Experts in cybersecurity frequently highlight healthcare-related entities as particularly vulnerable to cyberattacks due to the high value of the Private Information they collect and maintain.

507. The minimum information security standards applicable to Defendants are established by industry-accepted information security frameworks, including but not limited to: the NIST Cybersecurity Framework, the Center for Internet Security's Critical Security Controls (CIS CSC), and the HITRUST CSF, which are all established standards in reasonable cybersecurity readiness.

508. These frameworks represent established industry standards for healthcare-related entities. Had Defendants complied with these accepted standards, the hackers would not have been able to exploit Defendants vulnerabilities and carry out the Data Breach.

The Data Breach Caused Its Victims Harm

509. As a result of Defendants' ineffective and inadequate data security practices, the Data Breach, and the foreseeable consequences of Private Information ending up in the hands of criminals, the risk of identity theft to the Plaintiffs and Class members has materialized and is imminent. Consequently, Plaintiffs and Class members have sustained actual and imminent injuries and damages, including: (i) invasion of privacy; (ii) theft of their Private Information; (iii) fraud and identity theft from the misuse of their stolen Private Information; (iv) lost or diminished value of their Private Information; (v) lost time and opportunity costs associated with attempting to mitigate the effects of the Data Breach; (vi) emotional and mental distress and anguish; (vii) statutory damages; (viii) nominal damages; and (ix) the continued and increased risk to their Private Information, which remains in Defendants' possession and is subject to further

unauthorized disclosures unless Defendants implement appropriate and adequate information security controls.

510. As discussed in more detail *supra*, the Private Information likely exposed in the Data Breach is highly valuable and sought after on illicit underground markets for use in committing identity theft and fraud. Malicious actors use this data to access bank accounts, credit cards, and social media accounts, among other things.

511. The unencrypted Private Information of Plaintiffs and Class members will almost certainly be, if it has not already been, distributed through illicit underground criminal networks, including being sold on the dark web, as that is the *modus operandi* of the financially motivated hackers that perpetrated the Data Breach. Unencrypted Private Information may also fall into the hands of companies that will use the detailed Private Information for targeted marketing without the approval of Plaintiffs and Class members.

512. Plaintiffs and Class members therefore have suffered injury and face an imminent, substantial risk of further injuries like identity theft and related cybercrimes.

513. Malicious actors have also been known to wait years before using the Private Information, or they may re-use it to commit several cybercrimes, according to the GAO. And fraudulent use of data may continue for years after its sale or publication. As a result, the GAO concluded that studies that try to measure harms from data breaches "cannot necessarily rule out all future harm."[59]

514. Because of these injuries resulting from the Data Breach, Plaintiffs and Class members suffer and continue to suffer economic loss and actual harm, including:

- invasion of privacy;

[59] GAO Report, n.25, *supra*.

- disclosure or confidential information to a third party without consent;
- loss of the value of explicit and implicit promises of data security;
- identity fraud and theft; anxiety, loss of privacy, and emotional distress;
- the cost of detection and prevention measures for identity theft and unauthorized financial account and health insurance or health services use;
- lowered credit scores from credit inquiries;
- unauthorized charges;
- diminution of value of PII and PHI;
- loss of use of financial account funds and costs associated with inability to obtain money from their accounts or being limited in the amounts they were permitted to obtain from accounts, including missed payments on bills and loans, late charges and fees, and adverse effects on their credit;
- costs of credit and health insurance/health care services monitoring, identity theft production services, and credit freezes;
- costs associated with loss of time or productivity or enjoyment of one's life from the time required to mitigate and address consequences and future consequences of the Data Breach, such as searching for fraudulent activity, imposing withdrawal and purchase limits, as well as the stress and nuisance of Data Breach repercussions;
- increased suspicious and unauthorized spam emails, text messages, and phone calls for purposes of facilitating phishing and other hacking intrusions; and

- imminent, continued, and certainly impending injury flowing from the potential fraud and identity theft posed by the unauthorized possession of data by third parties.

Future Cost of Credit and Identity Theft Monitoring Is Reasonable and Necessary

515. For the reasons described *supra*, criminals will exploit this Private Information for identity theft crimes, such as opening bank accounts in victims' names for purchases or money laundering, filing fraudulent tax returns, securing loans or lines of credit, or submitting false unemployment claims, and fraudulently using health insurance or obtaining health care services or pharmaceutical products.

516. Such fraud may go undetected until debt collection calls commence months, or even years, later. An individual may not know that their Private Information was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

517. Consequently, Plaintiffs and Class members are at an increased risk of fraud and identity theft for many years into the future.

518. The retail cost of credit monitoring and identity theft monitoring can cost around $200 a year per individual. This is reasonable and necessary cost to monitor to protect Plaintiffs and Class members from the risk of identity theft that arose from the Data Breach.

CLASS ACTION ALLEGATIONS

519. Pursuant to Fed. R. Civ. P. 23(a), 23(b)(1), 23(b)(2), 23(b)(3), 23(c)(4) and/or 23(c)(5), Plaintiffs propose the following "Class" definition, subject to amendment as appropriate:

Nationwide Class:
All individuals residing in the United States and its territories whose Private Information was accessed and/or acquired by an unauthorized party as a result of the Data Breach that occurred in or about February 2024, including all persons who were sent a notice of the Data Breach (the "Class").

520. Plaintiffs also seek certification of the following statewide Subclasses (collectively, "Subclasses"), defined as follows and subject to amendment as appropriate:

Alabama Subclass:
All individuals residing in the state of Alabama whose Private Information was accessed and/or acquired by an unauthorized party as a result of the Data Breach that occurred in or about February 2024, including all persons who were sent a notice of the Data Breach.

Arizona Subclass:
All individuals residing in the state of Arizona whose Private Information was accessed and/or acquired by an unauthorized party as a result of the Data Breach that occurred in or about February 2024, including all persons who were sent a notice of the Data Breach.

Arkansas Subclass:
All individuals residing in the state of Arkansas whose Private Information was accessed and/or acquired by an unauthorized party as a result of the Data Breach that occurred in or about February 2024, including all persons who were sent a notice of the Data Breach.

California Subclass:
All individuals residing in the state of California whose Private Information was accessed and/or acquired by an unauthorized party as a result of the Data Breach that occurred in or about February 2024, including all persons who were sent a notice of the Data Breach.

Connecticut Subclass:
All individuals residing in the state of Connecticut whose Private Information was accessed and/or acquired by an unauthorized party as a result of the Data Breach that occurred in or about February 2024, including all persons who were sent a notice of the Data Breach.

Florida Subclass:
All individuals residing in the state of Florida whose Private Information was accessed and/or acquired by an unauthorized party as a result of the Data Breach that occurred in or about February 2024, including all persons who were sent a notice of the Data Breach.

Illinois Subclass:
All individuals residing in the state of Illinois whose Private Information was accessed and/or acquired by an unauthorized party as a result of the Data Breach that occurred in or about February 2024, including all persons who were sent a notice of the Data Breach.

Indiana Subclass:
All individuals residing in the state of Indiana whose Private Information was accessed and/or acquired by an unauthorized party as a result of the Data Breach that occurred in or about February 2024, including all persons who were sent a notice of the Data Breach.

Louisiana Subclass:
All individuals residing in the state of Louisiana whose Private Information was accessed and/or acquired by an unauthorized party as a result of the Data Breach that occurred in or about February 2024, including all persons who were sent a notice of the Data Breach.

Missouri Subclass:
All individuals residing in the state of Missouri whose Private Information was accessed and/or acquired by an unauthorized party as a result of the Data Breach that occurred in or about February 2024, including all persons who were sent a notice of the Data Breach.

Montana Subclass:
All individuals residing in the state of Montana whose Private Information was accessed and/or acquired by an unauthorized party as a result of the Data Breach that occurred in or about February 2024, including all persons who were sent a notice of the Data Breach.

New York Subclass:
All individuals residing in the state of New York whose Private Information was accessed and/or acquired by an unauthorized party as a result of the Data Breach that occurred in or about February 2024, including all persons who were sent a notice of the Data Breach.

North Carolina Subclass:
All individuals residing in the state of North Carolina whose Private Information was accessed and/or acquired by an unauthorized party as a result of the Data Breach that occurred in or about February 2024, including all persons who were sent a notice of the Data Breach.

Ohio Subclass:
All individuals residing in the state of Ohio whose Private Information was accessed and/or acquired by an unauthorized party as a result of the Data Breach

that occurred in or about February 2024, including all persons who were sent a notice of the Data Breach.

Pennsylvania Subclass:
All individuals residing in the state of Pennsylvania whose Private Information was accessed and/or acquired by an unauthorized party as a result of the Data Breach that occurred in or about February 2024, including all persons who were sent a notice of the Data Breach.

South Dakota Subclass:
All individuals residing in the state of South Dakota whose Private Information was accessed and/or acquired by an unauthorized party as a result of the Data Breach that occurred in or about February 2024, including all persons who were sent a notice of the Data Breach.

521. Excluded from the Class and Subclasses are the following individuals and/or entities: Cencora and Cencora's parents, subsidiaries, affiliates, officers and directors, and any entity in which Cencora has a controlling interest; Lash Group and Lash Group's parents, subsidiaries, affiliates, officers and directors, and any entity in which Lash Group has a controlling interest; the parents, subsidiaries, affiliates, and officers and directors of any entity that issued a data breach notification letter in connection with the Data Breach; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; and all judges assigned to hear any aspect of this litigation, members of their immediate families, and chambers staff.

522. Plaintiffs reserve the right to amend the definitions of the Class or Subclasses or add additional Classes or Subclasses.

523. Numerosity: The Class and Subclasses are so numerous that joinder is impracticable, if not completely impossible. Although the precise number of individuals is currently unknown to Plaintiffs and exclusively in the possession of Cencora, at least 1.4 million individuals were impacted. The Class and Subclasses are readily identifiable within and ascertainable from Cencora's records, and Cencora, the Drug Companies, and other entities have

already identified many of these individuals (as evidenced by sending them breach notification letters). The actual number of victims likely is much higher considering that Cencora has serviced over 18 million customers to date.[60]

524. Commonality: Common questions of law and fact exist as to all members of the Class and Subclasses and predominate over any questions affecting solely individual members of the Class. Among the questions of law and fact common to the Class and Subclasses that predominate over questions which may affect individual Class and Subclass members, including the following:

a. Whether and to what extent Defendants had a duty to protect the Private Information of Plaintiffs and Class and Subclass members;

b. Whether Defendants had respective duties not to disclose the Private Information of Plaintiffs and Class members to unauthorized third parties;

c. Whether Defendants had duties not to use the Private Information of Plaintiffs and Class members for non-business purposes;

d. Whether Defendants unlawfully used, maintained, lost, or disclosed Plaintiffs' and Class members' Private Information;

e. Whether Defendants failed to adequately safeguard the Private Information of Plaintiffs and Class members;

f. Whether Defendants knew or should have known that their data security systems and monitoring processes were deficient;

g. Whether and when Defendants actually learned of the Data Breach;

[60] Amy Clark, *Major Pharmaceutical Companies Hit by Data Breach Linked to Cencora Cyberattack*, TECHREPORT (Jan. 7, 2025), https://techreport.com/news/major-pharmaceutical-companies-data-breach-cencora-cyberattack/.

h. Whether Defendants adequately, promptly, and accurately informed Plaintiffs and Class members that their Private Information had been compromised;

i. Whether Defendants violated the law by failing to promptly notify Plaintiffs and Class members that their Private Information had been compromised;

j. 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;

k. Whether Defendants adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

l. Whether Defendants' conduct was negligent;

m. Whether Defendants were unjustly enriched by unlawfully retaining a benefit conferred upon them by Plaintiffs and Class members;

n. Whether Plaintiffs and Class members are entitled to actual damages, statutory damages, and/or nominal damages as a result of Defendants' wrongful conduct;

o. Whether Plaintiffs and Class members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach.

525. Typicality: Plaintiffs' claims are typical of the claims of the Class. Plaintiffs, like all proposed members of the Class, had Private Information compromised in the Data Breach. Plaintiffs and Class members were injured by the same wrongful acts, practices, and omissions committed by Defendants, as described herein. Plaintiffs' claims therefore arise from the same practices or course of conduct that give rise to the claims of all Class members.

526. Policies Generally Applicable to the Class: This class action is also appropriate for certification because Defendants acted or refused to act on grounds generally applicable to the

Class, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class members and making final injunctive relief appropriate with respect to the Class as a whole. Defendants' policies challenged herein apply to and affect Class members uniformly and Plaintiffs' challenges of these policies hinge on Defendants' conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiffs.

527. Adequacy: Plaintiffs will serve as fair and effective representatives for the Class members, possessing no conflicting interests that would hinder the protection of their rights. The relief sought by the Plaintiffs aligns with the collective interests of the Class, without any adverse implications for its members. The infringements upon the Plaintiffs' rights and the damages incurred are emblematic of those experienced by other Class members. Moreover, Plaintiffs have engaged legal counsel adept in navigating intricate class action and data breach litigation, demonstrating a commitment to vigorously pursue this case.

528. Superiority and Manageability: The class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of Class members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain Class members, who could not individually afford to litigate a complex claim against large corporations, like Defendants. Further, even for those Class members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

529. The nature of this action and the nature of laws available to Plaintiffs and Class members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiffs and Class members for the wrongs alleged because Defendants would necessarily gain an unconscionable advantage since they would be able to exploit and overwhelm the limited resources of each individual Class member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiffs were exposed is representative of that experienced by the Class and will establish the right of each Class member to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

530. The litigation of the claims brought herein is manageable. Defendants' uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class members demonstrate that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

531. Adequate notice can be given to Class members directly using information maintained in Defendants' records.

532. Unless a Class-wide injunction is issued, Defendants may continue in their failure to properly secure the Private Information of Class members, Defendants may continue to refuse to provide proper notification to Class members regarding the Data Breach, and Defendants may continue to act unlawfully as set forth in this Complaint.

533. Further, Defendants have acted on grounds that apply generally to the Class as a whole, so that class certification, injunctive relief, and corresponding declaratory relief are appropriate on a class-wide basis.

534. Similarly, specific issues outlined above warrant certification as they entail distinct yet shared concerns pivotal to advancing the resolution of this case and the interests of all parties involved. These issues include, but are not confined to:

a. Whether the Defendants failed to promptly notify both Plaintiffs and the Class about the Data Breach;

b. Whether the Defendants bore a legal responsibility to exercise due diligence in the acquisition, storage, and protection of Private Information belonging to Plaintiffs and the Class;

c. Whether the security measures implemented by Defendants to safeguard their data systems aligned with industry best practices endorsed by data security experts;

d. Whether Defendants' omission of adequate protective security measures amounted to negligence;

e. Whether Defendants neglected to undertake commercially reasonable measures to secure Private Information; and

f. Whether adherence to data security recommendations outlined by the FTC, by HIPAA, and those advocated by data security experts could have feasibly prevented the occurrence of the Data Breach.

CAUSES OF ACTION
COUNT I
Negligence
On Behalf of Plaintiffs and the Class

535. Plaintiffs re-allege and incorporate by reference paragraphs 1-534 as if fully set forth herein.

536. Plaintiffs bring this claim individually and on behalf of the Class against Defendants, and, in the alternative, on behalf of the State Subclasses under the laws of their

respective home states.

537. Defendants require consumers, including Plaintiffs and Class members, to submit non-public Private Information, either directly or indirectly, in the ordinary course or providing their services.

538. Defendants gathered and stored the Private Information of Plaintiffs and Class members as part of their business of providing their services, which services affect commerce.

539. Plaintiffs and Class members entrusted Defendants with their Private Information, expecting that Defendants would protect and secure it.

540. Defendants had full knowledge of the sensitivity of the Private Information and the types of harm that Plaintiffs and Class members could and would suffer if the Private Information were wrongfully disclosed.

541. By voluntarily undertaking the responsibility to collect, store, share, and use this data for commercial gain, Defendants assumed a duty of care to employ reasonable measures to secure and safeguard their computer systems and the Private Information of Class members contained within them. This duty included employing reasonable measures to prevent unauthorized disclosure and protect the information from theft. Additionally, Defendants were responsible for implementing processes to detect security breaches promptly and to notify affected individuals expeditiously in the event of a data breach.

542. Defendants had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

543. Defendants' duty to use reasonable security measures under HIPAA required

Defendants to "reasonably protect" confidential data from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 45 C.F.R. § 164.530(c)(l). Some or all of the healthcare and/or medical information at issue in this case constitutes "protected health information" within the meaning of HIPAA.

544. Defendants owed a duty of care to Plaintiffs and Class members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that their systems and networks adequately protected the Private Information.

545. Defendants' duty to employ reasonable security measures arose from the special relationship between Defendants and Plaintiffs and Class members. This relationship was established because the Plaintiffs and Class members entrusted Defendants with their confidential Private Information, both directly and indirectly as a necessary part of being consumers of the services provided by and the medications produced and/or distributed by Defendants.

546. Defendants also had a duty to exercise appropriate data deletion practices to remove former consumers', patients', and employees' Private Information they were no longer required to retain pursuant to regulations.

547. Defendants had, and continue to have, a duty to adequately disclose if the Private Information in their possession might have been compromised, the manner in which it was compromised, the specific types of data affected, and the timing of the breach. Such notice is necessary to enable the Plaintiffs and Class members to take steps to prevent, mitigate, and repair any identity theft or fraudulent use of their Private Information by third parties.

548. Defendants breached their duties under the FTC Act, HIPAA, the common law and other relevant standards, demonstrating negligence by failing to implement reasonable measures

to protect Class members' Private Information. Specific negligent actions and oversights by the Defendants include, but are not limited to:

a. Failing to implement and maintain reasonable technical and administrative information security controls to safeguard Class members' Private Information;

b. Inadequately monitoring the security of their networks and systems;

c. Allowing unauthorized access to Class members' Private Information;

d. Failing to promptly detect that Class members' Private Information had been compromised;

e. Neglecting to remove Private Information of former patients, customers, or employees that was no longer required to be retained according to regulations; and

f. Failing to promptly and adequately inform Class members about the occurrence and extent of the Data Breach, preventing them from taking appropriate measures to mitigate the risk of identity theft and other damages.

549. Defendants violated Section 5 of the FTC Act and HIPAA by failing to use reasonable measures to protect Private Information and not complying with applicable industry standards, as described in detail herein. Defendants' conduct was particularly unreasonable given the nature and amount of Private Information they obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiffs and the Class.

550. Plaintiffs and Class members were within the class of persons the Federal Trade Commission Act and HIPAA were intended to protect and the type of harm that resulted from the Data Breach was the type of harm that the statutes were intended to guard against.

551. Defendants' violation of Section 5 of the FTC Act and HIPAA constitutes negligence.

552. A breach of security, unauthorized access, and resulting injury to Plaintiffs and the Class was reasonably foreseeable, particularly in light of the nature of the data Defendants collected and Defendants' inadequate security practices.

553. It was foreseeable that Defendants' failure to use reasonable measures to protect Class members' Private Information would result in injury to Class members. Further, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches in the healthcare industry.

554. Defendants had full knowledge of the sensitivity of the Private Information and the types of harm that Plaintiffs and the Class could and would suffer if the Private Information were wrongfully disclosed.

555. Plaintiffs and the Class were the foreseeable and probable victims of any inadequate security practices and procedures. Defendants knew or should have known of the inherent risks in collecting and storing the Private Information of Plaintiffs and the Class, the critical importance of providing adequate security of that Private Information, and the necessity for encrypting Private Information stored on Defendants' systems or transmitted through third party systems.

556. It was thus foreseeable that the failure to adequately safeguard Class members' Private Information would lead to one or more forms of harm or injury to the Class members.

557. Plaintiffs and the Class had no ability to protect their Private Information that was in, and possibly remains in, Defendants' possession.

558. Defendants were in a position to protect against the harm suffered by Plaintiffs and the Class as a result of the Data Breach.

559. Defendants' duty extended to protecting Plaintiffs and the Class from the risk of

foreseeable criminal conduct of third parties, which has been recognized in situations where the actor's own conduct or misconduct exposes another to the risk or defeats protections put in place to guard against the risk, or where the parties are in a special relationship.

560. Defendants have admitted that the Private Information of Plaintiffs and the Class was wrongfully lost and disclosed to unauthorized third persons as a result of the Data Breach.

561. But for Defendants' wrongful and negligent breach of duties owed to Plaintiffs and the Class, the Private Information of Plaintiffs and the Class would not have been compromised.

562. There is a close causal connection between Defendants' failure to implement security measures to protect the Private Information of Plaintiffs and the Class and the harm, or risk of imminent harm, suffered by Plaintiffs and the Class. The Private Information of Plaintiffs and the Class was accessed and exfiltrated as the proximate result of Defendants' failure to exercise reasonable care in safeguarding such Private Information by adopting, implementing, and maintaining appropriate security measures.

563. As a direct and proximate result of Defendants' negligence, Plaintiffs and the Class have suffered and will suffer injury, including the following injuries and damages: (i) invasion of privacy; (ii) theft of their Private Information; (iii) fraud and identity theft from the misuse of their stolen Private Information; (iv) lost or diminished value of Private Information; (v) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vi) emotional and mental distress and anguish; (vii) statutory damages; (viii) nominal damages; and (ix) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains in Defendants' possession and is subject to further unauthorized disclosures so long as

Defendants fail to undertake appropriate and adequate measures to protect the Private Information.

564. Additionally, as a direct and proximate result of Defendants' negligence, Plaintiffs and the Class have suffered and will suffer the continued risks of exposure of their Private Information, which remains in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fails to undertake appropriate and adequate measures to protect the Private Information in their continued possession.

565. Plaintiffs and Class members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

566. Plaintiffs and the Class are also entitled to injunctive relief, which should compel the Defendants to implement and maintain reasonable and adequate technical and administrative information security controls given the vast amounts of extremely sensitive Private Information they collect, process, and store.

COUNT II
Breach of Fiduciary Duty
On Behalf of Plaintiffs and the Class

567. Plaintiffs re-allege and incorporate by reference paragraphs 1-534 as if fully set forth herein.

568. Plaintiffs bring this claim individually and on behalf of the Class against Defendants, and, in the alternative, on behalf of the State Subclasses under the laws of their respective home states.

569. Plaintiffs and Class members gave their Private Information in confidence, directly or indirectly, to Defendants, which collected and stored the information to carry out patient access and assistance programs or other pharmaceutical, healthcare, or employment services, believing

that Defendants would protect that information. Plaintiffs and Class members would not have provided Cencora, directly or indirectly, with this information had they known it would not be adequately protected. Cencora's acceptance and storage of Plaintiffs' and Class members' Private Information on behalf of the Drug Companies and other similar or affiliated companies created a fiduciary relationship between Defendants as actual or implied agents of the Drug Company's and other similar or affiliated companies, on the one hand, and Plaintiffs and Class members, on the other hand. In light of this relationship, Defendants must act primarily for the benefit of the individuals whose Private Information Defendants collected and stored, which includes safeguarding and protecting Plaintiffs' and Class members' Private Information.

570. Cencora had a fiduciary duty to act for the benefit of Plaintiffs and Class members upon matters within the scope of their relationship. Defendants breached that duty by failing to properly protect the integrity of the system(s) containing Plaintiffs' and Class members' Private Information, failing to comply with the data security guidelines set forth by HIPAA, and otherwise failing to safeguard Plaintiffs' and Class members' Private Information that it collected and maintained.

571. As a direct and proximate result of Defendants' breaches of their fiduciary duties, Plaintiffs and Class members have suffered and will suffer injury, including the following injuries and damages: (i) invasion of privacy; (ii) theft of their Private Information; (iii) fraud and identity theft from the misuse of their stolen Private Information; (iv) lost or diminished value of Private Information; (v) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vi) emotional and mental distress and anguish; (vii) statutory damages; (viii) nominal damages; and (ix) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties

to access and abuse; and (b) remains in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the Private Information.

COUNT III
Unjust Enrichment
On Behalf of Plaintiffs and the Class

572. Plaintiffs re-allege and incorporate by reference paragraphs 1-534 as if fully set forth herein.

573. Plaintiffs bring this claim individually and on behalf of the Class against Defendants, and, in the alternative, on behalf of the State Subclasses under the laws of their respective home states.

574. Plaintiffs and Class members conferred a monetary benefit on Defendants. Specifically, they paid Defendants, either directly or indirectly, for the provision of medications and/or services and in so doing also provided Defendants with their Private Information. In exchange, Plaintiffs and Class members should have received from Defendants the services that were the subject of the transaction and should have had their Private Information protected with adequate data security.

575. Defendants knew that Plaintiffs and Class members conferred a benefit upon them and had accepted and retained that benefit by accepting and retaining the Private Information entrusted to them. Defendants profited from Plaintiffs' and Class members' retained data and used Plaintiffs' and Class members' Private Information for business purposes.

576. Defendants failed to secure Plaintiffs' and Class members' Private Information and, therefore, did not fully compensate Plaintiffs or Class members for the value that their Private Information provided.

577. Defendants acquired the Private Information through inequitable record retention, having failed to investigate and/or disclose the inadequate data security practices previously mentioned.

578. If Plaintiffs and Class members had known that Defendants would not use adequate data security practices, procedures, and protocols to adequately monitor, supervise, and secure their Private Information, they would not have entrusted their Private Information to Defendants or obtained services from Defendants.

579. Plaintiffs and Class members have no adequate remedy at law.

580. Defendants enriched themselves by saving the costs they reasonably should have expended on data security measures to secure Plaintiffs' and Class members' Private Information. Instead of providing a reasonable level of security that would have prevented the hacking incident, Defendants calculated to increase their own profit at the expense of Plaintiffs and Class members by utilizing cheaper, ineffective security measures and diverting those funds to their own profit. Plaintiffs and Class members, on the other hand, suffered as a direct and proximate result of Defendants' decision to prioritize their own profits over the requisite security and the safety of Plaintiffs' and Class members Private Information.

581. Under the circumstances, it would be unjust for Defendants to be permitted to retain any of the benefits that Plaintiffs and Class members conferred upon them.

582. As a direct and proximate result of Defendants' conduct, Plaintiffs and Class members have suffered and will suffer injury, including the following injuries and damages: (i) invasion of privacy; (ii) theft of their Private Information; (iii) fraud and identity theft from the misuse of their stolen Private Information; (iv) lost or diminished value of Private Information; (v) lost time and opportunity costs associated with attempting to mitigate the actual consequences

of the Data Breach; (vi) emotional and mental distress and anguish; (vii) statutory damages; (viii) nominal damages; and (ix) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the Private Information.

583. Plaintiffs and Class members are entitled to full refunds, restitution, and/or damages from Defendants and/or an order proportionally disgorging all profits, benefits, and other compensation obtained by Defendants from their wrongful conduct. This can be accomplished by establishing a constructive trust from which the Plaintiffs and Class members may seek restitution or compensation.

584. Plaintiffs and Class members may not have an adequate remedy at law against Defendants, and accordingly, they plead this claim for unjust enrichment in addition to, or in the alternative to, other claims pleaded herein.

COUNT IV
Violations of the California Consumer Privacy Act
California Civil Code § 1798.150 ("CCPA")
On Behalf of California Plaintiffs and the California Subclass

585. California Plaintiffs Margie Lopez, Amanda Tucker, and Tuan Nguyen ("California Plaintiffs"), individually and on behalf of the California Subclass, re-allege and incorporate by reference paragraphs 1-534 as if fully set forth herein.

586. Cal. Civ. Code § 1798.150(a), provides that "[a]ny consumer whose nonencrypted and nonredacted personal information, as defined in subparagraph (A) of paragraph (1) of subdivision (d) of Section 1798.81.5 . . . is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business's violation of the duty to implement and maintain

reasonable security procedures and practices appropriate to the nature of the information to protect the personal information may institute a civil action" for statutory damages, actual damages, injunctive relief, declaratory relief and any other relief the court deems proper.

587. Defendants violated the CCPA, Cal. Civ. Code § 1798.150, by failing to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect California Plaintiffs' and California Subclass members' nonencrypted Private Information. As a direct and proximate result, California Plaintiffs' and California Subclass members' nonencrypted and nonredacted Private Information was subject to unauthorized access and exfiltration, theft, or disclosure during the Data Breach.

588. Defendants are "businesses" under the meaning of Civil Code § 1798.140 because each is a "corporation, association, or other legal entity that is organized or operated for the profit or financial benefit of its shareholders or other owners" that "collects consumers' personal information" and is active "in the State of California" and "had annual gross revenues in excess of twenty-five million dollars ($25,000,000) in the preceding calendar year." Cal. Civil Code § 1798.140(d).

589. California Plaintiffs and California Subclass members are "consumers" as defined by Cal. Civ. Code § 1798.140(g) because they are natural persons who reside in California.

590. California Plaintiffs and California Subclass members seek injunctive or other equitable relief to ensure Defendants hereinafter adequately safeguard Private Information by implementing reasonable security procedures and practices. Such relief is particularly important because Defendants continue to hold Private Information, including California Plaintiffs' and California Subclass members' Private Information.

591. California Plaintiffs and California Subclass members have an interest in ensuring

that their Private Information is reasonably protected, and Defendants have demonstrated a pattern of failing to adequately safeguard this information.

592. Defendants long have had notice of California Plaintiffs' allegations, claims, and demands, including from the filing of numerous related actions against them arising from the Data Breach, the first of which was filed in or about May 2024. Further, Defendants possess the most knowledge of the underlying facts giving rise to the California Plaintiffs' allegations, so that any pre-suit notice would not put them in a better position to evaluate those claims.

593. In accordance with Cal. Civ. Code §1798.150(b), prior to the filing of this complaint, California Plaintiffs' counsel served Defendants with notice of their CCPA violations. Plaintiff Lopez sent Defendants notices consistent with the CCPA on or about June 7, 2024, and Plaintiffs Tucker and Nguyen sent Defendants similar notices on or about February 20, 2025. Based on information and belief, additional plaintiffs in related actions further provided Defendants with CCPA notices between May 2024 and present.

594. To date, Defendants have failed to take sufficient and reasonable measures to safeguard their data security systems and protect the California Plaintiffs' and California Subclass members' highly sensitive Private Information from unauthorized access. Defendants' failure to maintain adequate data protections subjected their nonencrypted and nonredacted sensitive Private Information to exfiltration and disclosure by malevolent actors.

595. The unauthorized access, exfiltration, theft, and disclosure of California Plaintiffs' and California Subclass members' Private Information was a result of Defendants' violations of their duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the Private Information.

596. Under Defendants' duty to protect Private Information, they were required to implement reasonable security measures to prevent and deter hackers from accessing the Private Information. These vulnerabilities existed and enabled unauthorized third parties to access and harvest customers' Private Information, evidence that Defendants have breached their duty. California Plaintiffs and the California Subclass members have suffered actual injury. Plaintiff Lopez and the California Subclass are entitled to damages in an amount to be proven at trial but in excess of the minimum jurisdictional requirement of this Court.

597. Defendants' violations of Cal. Civ. Code § 1798.150(a) are a direct and proximate result of the Data Breach.

598. Plaintiff Lopez and California Subclass members seek all monetary and non-monetary relief allowed by law, including actual or nominal damages; declaratory and injunctive relief, including an injunction barring Defendants from disclosing their Private Information without their consent; reasonable attorneys' fees and costs; and any other relief that is just and proper.

599. Plaintiff Lopez and California Subclass members are further entitled to the greater of statutory damages in an amount not less than $100 and not greater than $750 per consumer per incident or actual damages, whichever is greater. *See* Cal. Civ. Code § 1798.150(b).

600. At this time, Plaintiffs Tucker and Nguyen seek only injunctive relief in the form of an order enjoining Defendants from continuing to violate the CCPA.

601. If Defendants fail to agree to rectify the violations detailed above, Plaintiffs Tucker and Nguyen will amend their pleading to seek actual, punitive, and statutory damages, restitution, and any other relief the Court deems proper to redress Defendants' CCPA violations.

COUNT V
Violations of the California Unfair Competition Law
Cal. Bus. & Prof. Code § 17200 *et seq*. ("UCL")
On Behalf of California Plaintiffs and the California Subclass

602. California Plaintiffs, individually and on behalf of the California Subclass, re-allege and incorporate by reference paragraphs 1-534 as if fully set forth herein.

603. The California UCL prohibits any "unlawful" or "unfair" business act or practice, as defined by the UCL and relevant case law.

604. By reason of Defendants' above-described conduct, the resulting Data Breach, and the unauthorized disclosure of the California Plaintiffs' and California Subclass members' Private Information, Defendants engaged in unfair and unlawful business practices in violation of the UCL.

605. California Plaintiffs and California Subclass member suffered injury, in fact, and lost money or property as a result of Defendants' alleged violations of the UCL.

606. The acts and conduct of Defendants as alleged herein constitute a "business practice" within the meaning of the UCL.

Unlawful Prong

607. Defendants violated the unlawful prong of the UCL by violating, *inter alia*, the CCPA, CCRA, CMIA, HIPAA, and the FTC Act as alleged herein.

608. Defendants' conduct also undermines California public policy—as reflected in statutes like the California Information Practices Act, Cal. Civ. Code §§ 1798, *et seq.*, the CCPA concerning consumer privacy, the CMIA concerning medical privacy, and the CCRA concerning customer records—which seek to protect customer and consumer data and ensure that entities who solicit or are entrusted with personal data utilize reasonable security measures.

Unfair Prong

609. Defendants' acts and conduct also violate the unfair prong of the UCL because they offended public policy and constitutes immoral, unethical, oppressive, and unscrupulous activities that caused substantial injury. The gravity of Defendants' conduct outweighs any potential benefits attributable to such conduct and there were reasonably available alternatives to further Defendants' legitimate business interests, other than the conduct described herein.

610. Defendants' failure to utilize, and to disclose they do not utilize, industry standard data security practices, constitutes an unfair business practice under the UCL. Defendants' conduct is unethical, unscrupulous, and substantially injurious to California Plaintiffs and the California Subclass. While Defendants' competitors have spent the time and money necessary to appropriately safeguard their products, service, and customer information, Defendants have not—to the detriment of their customers, patients, employees, other affiliated persons, and competition.

611. As a result of Defendants' violations of the UCL, the California Plaintiffs and California Subclass members are entitled to injunctive relief including, but not limited to: (1) ordering that Defendants utilize strong industry standard data security measures for the collection, storage, and retention of Private Information; (2) ordering that Defendants, consistent with industry standard practices, engage third party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendants' systems on a periodic basis; (3) ordering that Defendants engage third party security auditors and internal personnel, consistent with industry standard practices, to run automated security monitoring; (4) ordering that Defendants audit, test, and train its security personnel regarding any new or modified procedures; (5) ordering that Defendants, consistent with industry standard practices, segment consumer data by, among other things, creating

firewalls and access controls so that if one area of Defendants' systems are compromised, hackers cannot gain access to other portions of those systems; (6) ordering that Defendants purge, delete, and destroy in a reasonably secure manner Class member data not necessary for its provisions of services; (7) ordering that Defendants, consistent with industry standard practices, conduct regular database scanning and security checks; (8) ordering that Defendants, consistent with industry standard practices, evaluate all software, systems, or programs utilized for collection and storage of sensitive Private Information for vulnerabilities to prevent threats to customers; (9) ordering that Defendants, consistent with industry standard practices, periodically conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and (10) ordering Defendants to meaningfully educate its customers about the threats they face as a result of the loss of their Private Information.

612. As a result of Defendants' violations of the UCL, the California Plaintiffs and California Subclass members have suffered injury in fact and lost money or property, as detailed herein. They agreed to transact with Defendants or otherwise spent money that they otherwise would not have made or spent, had they known the true state of affairs regarding Defendants' data security policies. Class members lost control over their Private Information and suffered a corresponding diminution in value of that Private Information, which is a property right. Class members lost money as a result of dealing with the fallout of and attempting to mitigate harm arising from the Data Breach.

613. California Plaintiffs request that the Court issue sufficient equitable relief to restore California Subclass members to the position they would have been in had Defendants not

engaged in violations of the UCL, including by ordering restitution of all funds that Defendants may have acquired as a result of those violations.

COUNT VI
Violations of the California Consumer Records Act
Cal. Civ. Code § 1798.80 *et seq*. ("CCRA")
On Behalf of California Plaintiffs and the California Subclass

614. California Plaintiffs, individually and on behalf of the California Subclass, re-allege and incorporate by reference paragraphs 1-534 as if fully set forth herein.

615. Under the CCRA, any "person or business that conducts business in California, and that owns or licenses computerized data that includes personal information" must "disclose any breach of the system following discovery or notification of the breach in the security of the data to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person." Cal. Civ. Code §1798.82. The disclosure must "be made in the most expedient time possible and without unreasonable delay" but disclosure must occur "immediately following discovery [of the breach], if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person." *Id.* (emphasis added).

616. The Data Breach constitutes a "breach of the security system" of Defendants. An unauthorized person acquired the personal, unencrypted information of the California Plaintiffs and California Subclass members.

617. Defendants knew that an unauthorized person had acquired the personal, unencrypted Private Information of the California Plaintiffs and California Subclass members, but waited to notify them. Given the severity of the Data Breach, this is an unreasonable delay.

618. Defendants' unreasonable delay prevented the California Plaintiffs and California Subclass members from taking appropriate measures from protecting themselves against harm.

619. As a direct or proximate result of Defendants' violations of Civil Code §§ 1798.81.5 and 1798.82, the California Plaintiffs and California Subclass members were (and continue to be) injured and have suffered (and will continue to suffer) the damages and harms described herein.

620. California Plaintiffs accordingly request that the Court enter an injunction requiring Defendants to implement and maintain reasonable security procedures, including, but not limited to: (1) ordering that Defendants utilize strong industry standard data security measures for the collection, storage, and retention of Private Information; (2) ordering that Defendants, consistent with industry standard practices, engage third party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendants' systems on a periodic basis; (3) ordering that Defendants engage third party security auditors and internal personnel, consistent with industry standard practices, to run automated security monitoring; (4) ordering that Defendants audit, test, and train their security personnel regarding any new or modified procedures; (5) ordering that Defendants, consistent with industry standard practices, segment consumer data by, among other things, creating firewalls and access controls so that if one area of Defendants' systems are compromised, hackers cannot gain access to other portions of those systems; (6) ordering that Defendants purge, delete, and destroy in a reasonably secure manner Class member data not necessary for their provisions of services; (7) ordering that Defendants, consistent with industry standard practices, conduct regular database scanning and security checks; (8) ordering that Defendants, consistent with industry standard practices, evaluate all software, systems, or programs utilized for collection and storage of sensitive Private Information for vulnerabilities to prevent threats to customers; (9) ordering that Defendants, consistent with industry standard practices, periodically

conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and (10) ordering Defendants to meaningfully educate their customers about the threats they face as a result of the loss of their Private Information.

621. The California Plaintiffs and California Subclass members seek relief under Cal. Civ. Code § 1798.84 including, but not limited to, actual damages, to be proven at trial, and injunctive relief.

COUNT VII
Violations of the California Confidentiality of Medical Information Act
Cal. Civ. Code §§ 56 *et seq*. ("CMIA")
On Behalf of California Plaintiffs and the California Subclass

622. California Plaintiffs, individually and on behalf of the California Subclass, re-allege and incorporate by reference paragraphs 1-534 as if fully set forth herein.

623. Defendants are subject to the requirements and mandates of the CMIA.

624. CMIA section 56.36 allows an individual to bring an action against a "person or entity who has negligently released confidential information or records concerning him or her in violation of this part."

625. As a direct result of their negligent failure to adequately protect the California Plaintiffs' and California Subclass members' Private Information, Defendants allowed for a data breach which released and actually exposed their Private Information criminals and/or unauthorized third parties.

626. The CMIA defines "medical information" as "any individually identifiable information, in electronic or physical form, in possession of or derived from a provider of health care ... regarding a patient's medical history, mental or physical condition, or treatment."

627. The CMIA defines individually identifiable information as "medical information [that] includes or contains any element of personal identifying information sufficient to allow identification of the individual, such as the [customers'] name, address, electronic mail address, telephone number, or social security number, or other information that, alone or in combination with other publicly available information, reveals the individual's identity." Cal. Civ. Code § 56.050.

628. Defendants are in possession of affected individuals' sensitive medical and other information. Further, the compromised data was individually identifiable because it was accompanied by elements sufficient to allow identification of the Plaintiffs by the third parties to whom the data was disclosed.

629. Defendants lawfully came into possession of the Plaintiffs' and class members' medical information and had a duty pursuant to Section 56.06 and 56.101 of the CMIA to maintain, store and dispose of the Plaintiffs' and class members' medical records in a manner that preserved their confidentiality. Sections 56.06 and 56.101 of the CMIA prohibit the negligent creation, maintenance, preservation, store, abandonment, destruction, or disposal of confidential medical information. Defendants further violated the CMIA by failing to use reasonable care, and in fact, negligently maintained the California Plaintiffs' and California Subclass members' medical information.

630. As a direct and proximate result of Defendants' violations of the CMIA, the California Plaintiffs and California Subclass members have been injured and are entitled to compensatory damages, punitive damages, and nominal damages of $1,000 for each of Defendants' violations of the CMIA, as well as attorneys' fees and costs pursuant to Cal. Civ. Code § 56.36.

COUNT VIII
Violation of Connecticut Unfair Trade Practices Act
Conn. Gen. Stat. §§ 42-110a *et seq*. ("CUTPA")
On Behalf of Connecticut Plaintiff and the Connecticut Subclass

631. Connecticut Plaintiff Celia Skorupski ("Connecticut Plaintiff"), individually and on behalf of the Connecticut Subclass, re-alleges and incorporates by reference paragraphs 1-534 as if fully set forth herein.

632. The CUTPA provides: "No person shall engage in unfair methods of competition and unfair . . . acts or practices in the conduct of any trade or commerce." Conn. Gen. Stat. § 42-110b(a).

633. Connecticut Plaintiff and each Connecticut Subclass member is a "person" as defined by Conn. Gen. Stat. § 42- 110a(3) and is a consumer of Defendants' services and thus qualifies as a "person who suffers any ascertainable loss of money or property, real or personal, as a result of the use or employment of a method, act or practice prohibited by section 42-110b" under Conn. Gen. Stat. § 42-110g.

634. Each Defendant is a "person" as defined by Conn. Gen. Stat. § 42-110a(3).

635. Defendants advertised, offered, or sold goods or services in Connecticut and therefore engaged in trade or commerce directly or indirectly affecting the people of Connecticut. Conn. Gen. Stat. § 42-110a(4).

636. Unfair acts or practices are those defined in CUTPA or by other Connecticut statutes, and are guided by the interpretation of the FTC Act.

637. The Connecticut data breach notification act, Conn. Gen. Stat. §36a701b, *et seq*., provides that failure to comply with the notice timelines constitutes a prohibited act or practice under CUTPA.

638. Specifically, Defendants collected and stored Connecticut Plaintiff's and the Connecticut's Subclass's Private Information. Defendants stored the Private Information in a knowingly unsafe and unsecured manner by, among other things, failing to dispose of data no longer needed for any legitimate business purpose, maintaining the data on an unsecured database in an unencrypted format, failing to adequately monitor activity on the servers containing Connecticut Plaintiff's and the Connecticut Subclass's Private Information, and failing to adequately segment the sensitive data from other parts of Defendants' servers and networks.

639. Similarly, Defendants deployed knowingly unreasonable data security measures that defied expert recommendations, industry standards, and statutory requirements for reasonable data security, including by, but not limited to:

a. Failing to implement and maintain reasonable technical and administrative information security controls to safeguard Subclass members' Private Information.

b. Inadequately monitoring the security of their networks and systems.

c. Allowing unauthorized access to Subclass members' Private Information.

d. Failing to promptly detect that Subclass members' Private Information had been compromised.

e. Neglecting to remove Private Information that was no longer required to be retained according to regulations.

f. Failing to promptly and adequately inform Subclass members about the occurrence and extent of the Data Breach, preventing them from taking appropriate measures to mitigate the risk of identity theft and other damages.

640. Defendants' failure to comply with basic data security necessary to protect any stored data, much less the sensitive Private Information Defendants stored constitutes immoral, unethical, oppressive, and unscrupulous conduct that caused substantial harm to Connecticut Plaintiff and the Connecticut Subclass. That is especially true because, despite failing to reasonably protect Connecticut Plaintiff's and the Connecticut Subclass's highly sensitive Private Information, upon information and belief, Defendants gained significant profit from that information. While Defendants profited from Connecticut Plaintiff's and the Connecticut Subclass's data, they failed to take the necessary measures to protect it, leaving Connecticut Plaintiff and the Connecticut Subclass at significant and foreseeable risk of harm.

641. As a result of those unlawful and unfair business practices, Connecticut Plaintiff's and the Connecticut Subclass's highly sensitive and private health and medical information was put at foreseeable risk of unauthorized access, theft, and acquisition. That risk materialized with the Data Breach, where hackers obtained and successfully exfiltrated the Private Information.

642. As a direct and proximate result of Defendants' inadequate security and the resulting Data Breach, Connecticut Plaintiff and the Connecticut Subclass suffered and will continue to suffer significant injuries, including, but not limited to: (i) invasion of privacy; (ii) theft of their Private Information; (iii) fraud and identity theft from the misuse of their stolen Private Information; (iv) lost or diminished value of Private Information due to loss of security, confidentiality, and privacy; (v) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vi) emotional and mental distress and anguish; (vii) statutory damages; (viii) nominal damages; and (ix) the continued and certainly increased risk to their Private Information, which: (a) remains inadequately secured and vulnerable to unauthorized access and abuse; and (b) remains in Defendants' possession and is

subject to further unauthorized disclosures so long as Defendants fails to undertake appropriate and adequate measures to protect the Private Information.

643. Connecticut Plaintiff and the Connecticut Subclass also remain at heightened risk of future injury because their information resides with Defendants and, further, because Defendants continue to gather new medical information on Connecticut Plaintiff and the Connecticut Subclass. Without the use of adequate data security, Connecticut Plaintiff and the Connecticut Subclass remain at a heightened and substantial risk that their Private Information will be subject to another data breach.

644. Connecticut Plaintiff and the Connecticut Subclass seek all monetary and non-monetary relief allowed by law, including any: economic damages; damages for emotional and mental anguish; nominal damages; enhanced or treble damages available under the law; court costs; reasonable and necessary attorneys' fees; injunctive relief; and any other relief available by law and to which the court deems proper.

COUNT IX
Violation of Illinois Consumer Fraud and Deceptive Business Practices Act
815 Ill. Comp. Stat. §§ 505 *et seq.* ("ICFA")
On Behalf of Illinois Plaintiffs and the Illinois Subclass

645. Illinois Plaintiffs Juan Anaya and Robert Angulo ("Illinois Plaintiffs"), individually and on behalf of the Illinois Subclass, re-allege and incorporate by reference paragraphs 1-534 as if fully set forth herein.

646. The ICFA makes unlawful certain acts by persons in the conduct of trade or commerce. 815 Ill. Comp. Stat. § 505/2. Violating the Illinois Personal Information Protection Act ("IPIPA"), 815 Ill. Comp. Stat. 530/1, *et seq*., is one such unlawful act. 815 Ill. Comp. Stat. 530/20.

647. The IPIPA requires "[a]ny data collector that owns or licenses personal information concerning an Illinois resident" to provide notice to the resident expediently and without unreasonable delay "that there has been a breach of the security of the system data following discovery or notification of the breach." 815 Ill. Comp. Stat. § 530/10.

648. Defendants are data collectors that own the personal information of Illinois's residents as defined by the IPIPA. 815 Ill. Comp. Stat. 530/5.

649. The IPIPA requires data collectors like Defendants that own or maintain "records that contain personal information concerning an Illinois resident" to "implement and maintain reasonable security measures to protect those records from unauthorized access, acquisition, destruction, use, modification, or disclosure." 815 Ill. Comp. Stat. § 530/45. Defendants failed to implement and maintain reasonable security measures as required by the statute.

650. Specifically, Defendants collected and stored Illinois Plaintiffs' and the Illinois Subclass's Private Information. Defendants stored the Private Information in a knowingly unsafe and unsecured manner by, among other things, failing to dispose of data no longer needed for any legitimate business purpose, maintaining the data on an unsecured database in an unencrypted format, failing to adequately monitor activity on the servers containing Illinois Plaintiffs' and the Illinois Subclass's Private Information, and failing to adequately segment the sensitive data from other parts of Defendants' servers and networks.

651. Similarly, Defendants deployed knowingly unreasonable data security measures that defied expert recommendations, industry standards, and statutory requirements for reasonable data security, including by, but not limited to:

a. Failing to implement and maintain reasonable technical and administrative information security controls to safeguard Subclass members' Private Information.

b. Inadequately monitoring the security of their networks and systems.

c. Allowing unauthorized access to Subclass members' Private Information.

d. Failing to promptly detect that Subclass members' Private Information had been compromised.

e. Neglecting to remove Private Information that was no longer required to be retained according to regulations.

f. Failing to promptly and adequately inform Subclass members about the occurrence and extent of the Data Breach, preventing them from taking appropriate measures to mitigate the risk of identity theft and other damages.

652. Consequently, Defendants took actions in violation of the IPIPA that caused substantial harm to Illinois Plaintiffs and the Illinois Subclass members. That is especially true because, despite failing to reasonably protect Illinois Plaintiffs' and the Illinois Subclass's highly sensitive Private Information, upon information and belief, Defendants gained significant profit from that Private Information. While Defendants profited from Illinois Plaintiffs' and the Illinois Subclass's Private Information, they failed to take the necessary measures to protect it, leaving Illinois Plaintiffs and the Illinois Subclass at significant and foreseeable risk of harm.

653. Illinois Plaintiffs' and the Illinois Subclass's highly sensitive Private Information was put at foreseeable risk of unauthorized access, theft, and acquisition. That risk materialized with the Data Breach, where hackers obtained and successfully exfiltrated the Private Information of over 1.4 million individuals.

654. Due to Defendants' inadequate security, the resulting Data Breach, and the unreasonably delayed notice, Illinois Plaintiffs and the Illinois Subclass suffered and will continue to suffer significant injuries, including, but not limited to: (i) invasion of privacy; (ii) theft of their

Private Information; (iii) fraud and identity theft from the misuse of their stolen Private Information; (iv) lost or diminished value of Private Information due to loss of security, confidentiality, and privacy; (v) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vi) emotional and mental distress and anguish; (vii) statutory damages; (viii) nominal damages; and (ix) the continued and certainly increased risk to their Private Information, which: (a) remains inadequately secured and vulnerable to unauthorized access and abuse; and (b) remains in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fails to undertake appropriate and adequate measures to protect the Private Information.

655. Illinois Plaintiffs and the Illinois Subclass also remain at heightened risk of future injury because their Private Information resides with Defendants and, further, because Defendants continue to gather new medical information on Illinois Plaintiffs and the Illinois Subclass. Without the use of adequate data security, Illinois Plaintiffs and the Illinois Subclass remain at a heightened and substantial risk that their Private Information will be subject to another data breach.

656. Illinois Plaintiffs and the Illinois Subclass seek all monetary and non-monetary relief allowed by law, including any: economic damages; damages for emotional and mental anguish; nominal damages; enhanced or treble damages available under the law; court costs; reasonable and necessary attorneys' fees; injunctive relief; and any other relief available by law and to which the court deems proper.

COUNT X
Violation of the Louisiana Database Security Breach Notification Law
La. R.S. 51:3701 *et seq*.
On Behalf of Louisiana Plaintiff and the Louisiana Subclass

657. Louisiana Plaintiff Marilyn Borne ("Louisiana Plaintiff"), individually and on

behalf of the Louisiana Subclass, re-alleges and incorporates by reference paragraphs 1-534 as if fully set forth herein.

658. The Louisiana Database Security Breach Notification Law provides that "[a]ny person that owns or licenses computerized data that includes personal information, or any agency that owns or licenses computerized data that includes personal information, shall, following discovery of a breach in the security of the system containing such data, notify any resident of the state whose Private Information was, or is reasonably believed to have been, acquired by an unauthorized person." La. R.S. 51:3704(C).

659. Defendants are persons that own maintain, and license Personal Information, within the meaning of La. R.S. 51:3704, about Louisiana Plaintiff and the Louisiana Subclass. Businesses that own or license computerized data that includes Private Information, including SSNs, medical information, and health information, are required to notify Louisiana residents when their Private Information has been acquired (or reasonably believed to have been acquired) "in the most expedient time possible and without unreasonable delay but not later than sixty days from the discovery of the breach" La. R.S. 51:3704(E).

660. Louisiana Plaintiff's and Louisiana Subclass members' Private Information includes the type of information covered by La. R.S. 51:3704.

661. Defendants became aware of the data breach on February 21, 2024. According to Defendants' own statements, notifications did not even begin to be mailed until at least May 2024. Although the Data Breach occurred in February 2024 and Defendants knew of it shortly thereafter, Defendants have not confirmed that they have fully provided the required written notice to the affected individuals.

662. Consequently, Louisiana Plaintiff and the Louisiana Subclass members did not

know they were impacted by the Data Breach until they received direct notice several months after the breach occurred. That notice is insufficient under Louisiana law.

663. By failing to properly disclose the Data Breach in a timely and accurate manner, Defendants violated La. R.S. 3704.

664. Due to Defendants' inadequate security, the resulting Data Breach, and the unreasonably delayed notice, Louisiana Plaintiff and the Louisiana Subclass suffered and will continue to suffer significant injuries, including, but not limited to: (i) invasion of privacy; (ii) theft of their Private Information; (iii) fraud and identity theft from the misuse of their stolen Private Information; (iv) lost or diminished value of Private Information; (v) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vi) emotional and mental distress and anguish; (vii) statutory damages; (viii) nominal damages; and (ix) the continued and certainly increased risk to their Private Information, which: (a) remains inadequately secured and vulnerable to unauthorized access and abuse; and (b) remains in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fails to undertake appropriate and adequate measures to protect the Private Information.

665. Louisiana Plaintiff and Louisiana Subclass members seek relief under La. R.S. 51:3705, including actual damages and injunctive relief.

COUNT XI
Violation of Louisiana Unfair Trade Practices Act
La. RS 51 §1405 *et seq*. ("LUTPA")
On Behalf of Louisiana Plaintiff and the Louisiana Subclass

666. Louisiana Plaintiff, individually and on behalf of the Louisiana Subclass, re-allege and incorporate by reference paragraphs 1-534 as if fully set forth herein.

667. The LUTPA prohibits any person from engaging in unfair methods of competition

and unfair acts or practices in the conduct of any trade or commerce. La. R.S. 51:1405 (A).

668. Any person that conducts business in the state or that owns or licenses computerized data that includes personal information, or any agency that owns or licenses computerized data that includes personal information, shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the Private Information from unauthorized access, destruction, use, modification, or disclosure. La. R.S. 51:3704(A).

669. Violation of the provisions of La. R.S. 51:3704(A) shall constitute an unfair act or practice under La. R.S. 51:1405(A).

670. Defendants violated LUTPA by engaging in conduct that constituted unfair acts or practices, by collecting and storing Plaintiff's and the Louisiana Subclass's Private Information in a knowingly unsafe and unsecured manner by, among other things, failing to dispose of data no longer needed for any legitimate business purpose, maintaining the data on an unsecured database in an unencrypted format, failing to adequately monitor activity on the servers containing Plaintiff's the Louisiana Subclass's Private Information, and failing to adequately segment the sensitive data from other parts of Defendants' servers and networks.

671. Similarly, Defendants deployed knowingly unreasonable data security measures that defied expert recommendations, industry standards, and statutory requirements for reasonable data security, including by, but not limited to:

a. Failing to implement and maintain reasonable technical and administrative information security controls to safeguard Subclass members' Private Information.

b. Inadequately monitoring the security of their networks and systems.

c. Allowing unauthorized access to Subclass members' Private Information.

d. Failing to promptly detect that Subclass members' Private Information had been compromised.

e. Neglecting to remove Private Information that was no longer required to be retained according to regulations.

f. Failing to promptly and adequately inform Subclass members about the occurrence and extent of the Data Breach, preventing them from taking appropriate measures to mitigate the risk of identity theft and other damages.

672. Consequently, Defendants took actions in violation of LUTPA that caused substantial harm to Louisiana Plaintiff and the Louisiana Subclass members. That is especially true because, despite failing to reasonably protect Louisiana Plaintiff's and Louisiana Subclass's highly sensitive Private Information, upon information and belief, Defendants gained significant profit from that Private Information. While Defendants profited from Louisiana Plaintiff's and the Louisiana Subclass's Private Information, they failed to take the necessary measures to protect it, leaving Louisiana Plaintiff and the Louisiana Subclass at significant and foreseeable risk of harm.

673. Louisiana Plaintiff and the Louisiana Subclass's highly sensitive and Private Information was put at foreseeable risk of unauthorized access, theft, and acquisition. That risk materialized with the Data Breach, where hackers obtained and successfully exfiltrated Private Information of over 1.4 million individuals.

674. Due to Defendants' inadequate security, the resulting Data Breach, and the unreasonably delayed notice, Louisiana Plaintiff and the Louisiana Subclass suffered and will continue to suffer significant injuries, including, but not limited to: (i) invasion of privacy; (ii)

theft of their Private Information; (iii) fraud and identity theft from the misuse of their stolen Private Information; (iv) lost or diminished value of Private Information; (v) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vi) emotional and mental distress and anguish; (vii) statutory damages; (viii) nominal damages; and (ix) the continued and certainly increased risk to their Private Information, which: (a) remains inadequately secured and vulnerable to unauthorized access and abuse; and (b) remains in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fails to undertake appropriate and adequate measures to protect the Private Information.

675. Louisiana Plaintiff and the Louisiana Subclass also remain at heightened risk of future injury because their Private Information resides with Defendants and, further, because Defendants continue to gather new medical information on Louisiana Plaintiff and the Louisiana Subclass. Without the use of adequate data security, Louisiana Plaintiff and the Louisiana Subclass remain at a heightened and substantial risk that their Private Information will be subject to another data breach.

676. Louisiana Plaintiff and the Louisiana Subclass seek all monetary and non-monetary relief allowed by law, including any: economic damages; damages for emotional and mental anguish; nominal damages; court costs; reasonable and necessary attorneys' fees; injunctive relief; and any other relief available by law and to which the court deems proper pursuant to La. R.S. 51:1409.

COUNT XII
Violation of North Carolina Unfair and Deceptive Trade Practices Act
N.C. Gen. Stat. § 75.1.1 *et seq.* ("NCUDTPA")
On Behalf of North Carolina Plaintiff and the North Carolina Subclass

677. North Carolina Plaintiff Kyle Reynolds ("North Carolina Plaintiff"), individually

and on behalf of the North Carolina Subclass, re-alleges and incorporates by reference paragraphs 1-534 as if fully set forth herein.

678. The NCUDTPA provides that "[u]nfair methods of competition in or affecting commerce, and unfair . . . acts or practices in or affecting commerce, are declared unlawful." N.C. Gen. Stat. Ann. § 75-1.1.

679. "[U]nfair methods of competition" is interpreted broadly to include acts that violate other laws and may include acts even if not specifically proscribed by some other law.

680. Defendants advertised, offered, or sold goods or services in North Carolina and engaged in trade or commerce directly or indirectly affecting the people of North Carolina, as defined by N.C. Gen. Stat. Ann. § 75-1.1(b).

681. Specifically, Defendants collected and stored North Carolina Plaintiff's and the North Carolina Subclass's Private Information. Defendants stored the Private Information in a knowingly unsafe and unsecured manner by, among other things, failing to dispose of data no longer needed for any legitimate business purpose, maintaining the data on an unsecured database in an unencrypted format, failing to adequately monitor activity on the servers containing North Carolina Plaintiff's and the North Carolina Subclass's information, and failing to adequately segment the sensitive data from other parts of Defendants' servers and networks. Similarly, Defendants deployed knowingly unreasonable data security measures that defied expert recommendations, industry standards, and statutory requirements for reasonable data security, including by, but not limited to:

a. Failing to implement and maintain reasonable technical and administrative information security controls to safeguard Subclass members' Private Information.

b. Inadequately monitoring the security of their networks and systems.

c. Allowing unauthorized access to Subclass members' Private Information.

d. Failing to promptly detect that Subclass members' Private Information had been compromised.

e. Neglecting to remove Private Information that was no longer required to be retained according to regulations.

f. Failing to promptly and adequately inform Subclass members about the occurrence and extent of the Data Breach, preventing them from taking appropriate measures to mitigate the risk of identity theft and other damages.

682. Consequently, Defendants took actions in violation of the NCUDTPA that caused substantial harm to North Carolina Plaintiff and the North Carolina Subclass members. That is especially true because, despite failing to reasonably protect North Carolina Plaintiff's and the North Carolina Subclass's highly sensitive Private Information, upon information and belief, Defendants gained significant profit from that Private Information. While Defendants profited from North Carolina Plaintiff's and the North Carolina Subclass's Private Information, they failed to take the necessary measures to protect it, leaving North Carolina Plaintiff and the North Carolina Subclass at significant and foreseeable risk of harm.

683. As a result of those unlawful and unfair business practices, North Carolina Plaintiff and the North Carolina Subclass's highly sensitive and private health and medical information was put at foreseeable risk of unauthorized access, theft, and acquisition. That risk materialized with the Data Breach, where hackers obtained and successfully exfiltrated the Private Information of over one hundred million patients.

684. As a direct and proximate result of Defendants' inadequate security and the resulting Data Breach, North Carolina Plaintiff and the North Carolina Subclass suffered and will

continue to suffer significant injuries, including, but not limited to: (i) invasion of privacy; (ii) theft of their Private Information; (iii) fraud and identity theft from the misuse of their stolen Private Information; (iv) lost or diminished value of Private Information; (v) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vi) emotional and mental distress and anguish; (vii) statutory damages; (viii) nominal damages; and (ix) the continued and certainly increased risk to their Private Information, which: (a) remains inadequately secured and vulnerable to unauthorized access and abuse; and (b) remains in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the Private Information.

685. North Carolina Plaintiff and the North Carolina Subclass also remain at heightened risk of future injury because their information resides with Defendants and, further, because Defendants continue to gather new medical information on North Carolina Plaintiff and the North Carolina Subclass. Without the use of adequate data security, North Carolina Plaintiff and the North Carolina Subclass remain at a heightened and substantial risk that their Private Information will be subject to another data breach.

686. North Carolina Plaintiff and the North Carolina Subclass seek all monetary and non-monetary relief allowed by law, including any: economic damages; damages for emotional and mental anguish; nominal damages; enhanced or treble damages available under the law; court costs; reasonable and necessary attorneys' fees; injunctive relief; and any other relief available by law and to which the court deems proper.

COUNT XIII
Violation of North Carolina Identity Theft Protection Act
N.C. Gen. Stat. § 75-60 *et seq*.
On Behalf of North Carolina Plaintiff and the North Carolina Subclass

687. North Carolina Plaintiff, individually and on behalf of the North Carolina Subclass, re-allege and incorporate by reference paragraphs 1-534 as if fully set forth herein.

688. In pertinent part, N.C. Gen. Stat. § 75-65 provides:

> Any business that owns or licenses Private Information of residents of North Carolina or any business that conducts business in North Carolina that owns or licenses Private Information in any form (whether computerized, paper, or otherwise) shall provide notice to the affected person that there has been a security breach following discovery or notification of the breach. The disclosure notification shall be made without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subsection (c) of this section, and consistent with any measures necessary to determine sufficient contact information, determine the scope of the breach and restore the reasonable integrity, security, and confidentiality of the data system.

689. N.C. Gen. Stat. § 14-113.20b defines Private Information as a person's first name or initial and last name in combination with and linked to any one or more of the following data elements that relate to a resident of this State:

a. Social security or employer taxpayer identification numbers, N.C. Gen. Stat. § 14-113.20(b)(1);

b. Drivers license, State identification card, or passport numbers, N.C. Gen. Stat. § 14-113.20(b)(2);

c. Financial account number, or credit card or debit card number, N.C. Gen. Stat. § 14-113.20(b)(3)-(6);

d. Personal Identification Code, electronic identification numbers, electronic mail names or addresses, Internet account numbers, or Internet identification names, digital signatures, N.C. Gen. Stat. § 14-113.20(b)(7)-(9);

e. "any other numbers or information that can be used to access a person's financial resources," N.C. Gen. Stat. § 14-113.20(b)(10); or

f. biometric data, fingerprints, passwords, legal surname prior to marriage, N.C. Gen. Stat. § 14-113.20(b)(11)-(14).

690. Defendants own, license and/or maintain computerized data that includes North Carolina Plaintiff's and North Carolina Subclass Members' Private Information.

691. Defendants' conduct, as alleged herein, violated the Identity Theft Protection Act of North Carolina, N.C. Gen. Stat. § 75-60.

692. Defendants were required, but failed, to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the cyber security incident described herein.

693. The Data Breach constituted a "Security breach" within the meaning of N.C. Gen. Stat. § 75-60.

694. The information compromised in the Data Breach constituted "personal identifying information" within the meaning of N.C. Gen. Stat. § 75-60.

695. Defendants violated N.C. Gen. Stat. § 75-60 by unreasonably delaying disclosure of the Data Breach to Plaintiff and Class members, whose personal identifying information was, or reasonably believed to have been, acquired by an unauthorized person.

696. Specifically, Defendants collected and stored North Carolina Plaintiff's and the North Carolina Subclass's Private Information. Defendants stored the Private Information in a knowingly unsafe and unsecured manner by, among other things, failing to dispose of data no longer needed for any legitimate business purpose, maintaining the data on an unsecured database in an unencrypted format, failing to adequately monitor activity on the servers containing North

Carolina Plaintiff's and the North Carolina Subclass's information, and failing to adequately segment the sensitive data from other parts of Defendants' servers and networks.

697. Defendants' failure to comply with basic data security necessary to protect any stored data, much less the significant Private Information Defendants stored, constitutes immoral, unethical, oppressive, and unscrupulous conduct that caused substantial harm to more than 1.4 million individuals. That is especially true because, despite failing to reasonably protect North Carolina Plaintiff's and the North Carolina Subclass's highly sensitive Private Information, upon information and belief, Defendants gained significant profit from that information. While Defendants profited from North Carolina Plaintiff's and the North Carolina Subclass's data, they failed to take the necessary measures to protect it, leaving North Carolina Plaintiff and the North Carolina Subclass at significant and foreseeable risk of harm.

698. Consequently, Defendants took actions in violation of the Identity Theft Protection Act of North Carolina.

699. As a result of those unlawful and unfair business practices, North Carolina Plaintiff and the North Carolina Subclass's highly sensitive and private health and medical information was put at foreseeable risk of unauthorized access, theft, and acquisition. That risk materialized with the Data Breach, where hackers obtained and successfully exfiltrated the Private Information of over one hundred million patients.

700. Due to Defendants' inadequate security, the resulting Data Breach, and the unreasonably delayed notice, North Carolina Plaintiff and the North Carolina Subclass suffered and will continue to suffer significant injuries, including, but not limited to: (i) invasion of privacy; (ii) theft of their Private Information; (iii) fraud and identity theft from the misuse of their stolen Private Information; (iv) lost or diminished value of Private Information due to loss

of security, confidentiality, and privacy; (v) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vi) emotional and mental distress and anguish; (vii) statutory damages; (viii) nominal damages; and (ix) the continued and certainly increased risk to their Private Information, which: (a) remains inadequately secured and vulnerable to unauthorized access and abuse; and (b) remains in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fails to undertake appropriate and adequate measures to protect the Private Information.

701. North Carolina Plaintiff and the North Carolina Subclass also remain at heightened risk of future injury because their information resides with Defendants and, further, because Defendants continue to gather new medical information on North Carolina Plaintiff and the North Carolina Subclass. Without the use of adequate data security, North Carolina Plaintiff and the North Carolina Subclass remain at a heightened and substantial risk that their Private Information will be subject to another data breach.

702. North Carolina Plaintiff and the North Carolina Subclass seek all monetary and non-monetary relief allowed by law, including any: economic damages; damages for emotional and mental anguish; nominal damages; enhanced or treble damages available under the law; court costs; reasonable and necessary attorneys' fees; injunctive relief; and any other relief available by law and to which the court deems proper.

COUNT XIV
Declaratory Judgment
On Behalf of Plaintiffs and the Class

703. Plaintiffs re-allege and incorporate by reference paragraphs 1-534 as if fully set forth herein.

704. Plaintiffs bring this claim individually and on behalf of the Class against Defendants.

705. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201 *et seq.*, this Court is authorized to declare rights, status, and other legal relations, and such declarations shall have the force and effect of a final judgment or decree. Furthermore, the Court has broad authority to restrain acts, as here, that are tortious and violate the terms of the federal and state statutes described in this complaint.

706. An actual controversy has arisen in the wake of the Data Breach regarding Plaintiffs' and Class members' Private Information and whether Defendants are currently maintaining data security measures adequate to protect Plaintiffs and Class members from further data breaches that compromise their Private Information. Plaintiffs allege that Defendants' data security measures remain inadequate, contrary to Defendants' assertion that they have confirmed the security of their networks. Furthermore, Plaintiffs and Class members continue to suffer injury as a result of the compromise of Private Information and remain at imminent risk that further compromises of Private Information will occur in the future.

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

a. Defendants owe a legal duty to secure Private Information and to timely notify patients or any individuals impacted of a data breach under the common law, Section 5 of the FTC Act, HIPAA, and various state statutes; and

b. Defendants continue to breach their legal duty by failing to employ reasonable measures to secure consumers' Private Information.

708. This Court also should issue corresponding prospective injunctive relief requiring Defendants to, at minimum (1) disclose, expeditiously, the full nature of the Data Breach and the types of Private Information accessed, obtained, or exposed by the hackers; (2) implement improved data security practices to reasonably guard against future breaches of Plaintiffs' and Class members' Private Information possessed by Defendants; and (3) provide, at their own expense, all impacted victims with lifetime identity theft protection services.

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

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

711. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach at Defendants, thus eliminating the additional injuries that would result to Plaintiffs and Class members whose confidential information would be further compromised.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and the Class set forth herein, respectfully requests the following relief:

A. Certifying this action as a class action pursuant to Rule 23, certifying the Class as requested herein, designating Plaintiffs as Class Representatives, and appointing Plaintiffs' counsel as Class Counsel;

B. Awarding Plaintiffs and the Class equitable relief enjoining Defendants from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of the Private Information of Plaintiffs and Class members;

C. Awarding injunctive relief requested by Plaintiffs, including injunctive and other equitable relief as is necessary to protect the interests of Plaintiffs and Class members, including but not limited to an order:

i. requiring Defendants to conduct regular database scanning and securing checks;

ii. requiring Defendants to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling personal identifying information, as well as protecting the personal identifying information of Plaintiffs and Class members;

iii. requiring Defendants to implement a system of tests to assess their respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Defendants' policies, programs, and systems for protecting personal identifying information;

iv. requiring Defendants to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendants' information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

v. requiring Defendants to implement logging and monitoring programs sufficient to track traffic to and from Defendants' servers; and

vi. for a period of 10 years, appointing a qualified and independent third-party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendants' compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court's final judgment;

D. Awarding Plaintiffs and Class members damages, including actual, nominal, statutory, consequential, and punitive damages, for each cause of action as allowed by law in an amount to be determined at trial;

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

F. Awarding Plaintiffs the costs and disbursements of the action, along with reasonable attorney's fees, costs, and expenses;

G. Awarding Plaintiffs and the Class pre-judgment and post-judgment interest at the maximum legal rate;

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

I. Granting all other such relief as this Court deems just and proper.

DEMAND FOR JURY TRIAL

Plaintiffs hereby demand a trial by jury on all claims so triable.

Date: February 25, 2025

Respectfully submitted,

/s/ Andrew W. Ferich
Andrew W. Ferich (PA Bar No. 313696)
AHDOOT & WOLFSON, PC
201 King of Prussia Road, Suite 650
Radnor, PA 19087
Tel: (310) 474-9111
Fax: (310) 474-8585
aferich@ahdootwolfson.com

Erin Green Comite (admitted *pro hac vice*)
SCOTT+SCOTT
ATTORNEYS AT LAW LLP
156 S. Main Street
P.O. Box 192
Colchester, CT 06415
Tel: (860) 537-5537
Fax: (860) 537-4432
ecomite@scott-scott.com

Jeannine M. Kenney (PA Bar No. 307635)
HAUSFELD LLP
325 Chestnut Street, Suite 900
Philadelphia, PA 19106
Tel: (215) 985-3270
Fax: (215) 985-3271
jkenney@hausfeld.com

Shauna Itri (PA Bar No. 201611)
SEEGER WEISS LLP
325 Chestnut Street, Suite 917
Philadelphia, PA 19106
Tel: (215) 553-7981
Fax: (215) 851-8029
sitri@seegerweiss.com

Interim Co-Lead Class Counsel for Plaintiffs and the Putative Class