UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF PENNSYLVANIA

MICHAEL COGGINS, ELIZABETH FAGOT, and BRIDGET REARDON, *on behalf of themselves and all others similarly situated*, Plaintiffs, v. CENCORA, INC., THE LASH GROUP, LLC, BRISTOL MYERS SQUIBB COMPANY, and BRISTOL MYERS SQUIBB PATIENT ASSISTANCE FOUNDATION, INC. Defendants.	Case No. 2:24-cv-3554 **COMPLAINT – CLASS ACTION** **JURY TRIAL DEMANDED**

Plaintiffs Michael Coggins, Elizabeth Fagot, and Bridget Reardon ("Plaintiffs"), by and through their undersigned counsel, hereby file this Class Action Complaint, on behalf of themselves and all others similarly situated, against Defendants Cencora, Inc. ("Cencora"), The Lash Group, LLC ("Lash Group"), and Bristol Myers Squibb Company and Bristol Myers Squibb Patient Assistance Foundation, Inc. (collectively, "BMS") (all collectively, "Defendants"). Plaintiffs base the following allegations upon information and belief, investigation of counsel, and their own personal knowledge.

NATURE OF THE ACTION

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

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

3. The harm resulting from a data privacy breach manifests in a number of ways, including identity theft and financial fraud, and the exposure of a person's PII or PHI through a data breach ensures that such person will be at a substantially increased and certainly impending risk of identity theft crimes compared to the rest of the population, potentially for the rest of their lives. Mitigating that risk – to the extent it is even possible to do so – requires individuals to devote significant time and money to closely monitor their credit, financial accounts, health records, and email accounts, and take a number of additional prophylactic measures.

4. Cencora is a pharmaceutical corporation that provides services related to drug distribution, specialty pharmacy, consulting, and clinical trial support.[1]

5. Bristol-Myers Squibb Company is an multinational pharmaceutical company that manufactures prescription pharmaceuticals and biologics for consumers.

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

7. In order to provide these services to their clients, Defendants are entrusted with consumer and patient PII and PHI. For example, Cencora and Lash Group manage the patient support and

---

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

[2] *Lash Group Notice of Data Security Incident.*, THE LASH GROUP, https://www.lashgroup.com/#:~:text=We%20pair%20advanced%20technologies%20withevery%20step%20of%20the%20way.

access programs of Bristol Myers Squibb Company and Bristol Myers Squibb Patient Assistance Foundation, Inc., and as a result, gained access to BMS patients' PII and PHI.

8. As Defendants are or should have been aware, this type of personal and sensitive data is highly targeted by hackers who seek to exploit that data for nefarious purposes. In the wrong hands, these types of sensitive data may be wielded to cause significant harm to Plaintiffs and the Class Members.

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

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

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

---

[3] Toulas, *supra* note 1.

[4] *See* Novartis Pharmaceuticals Corporation, *Submitted Breach Notification Sample*, OFFICE OF THE ATTORNEY GENERAL, https://oag.ca.gov/ecrime/databreach/reports/sb24-585783 (last visited Jul. 29, 2024); Bayer Corporation, *Submitted Breach Notification Sample*, OFFICE OF THE ATTORNEY GENERAL, https://oag.ca.gov/ecrime/databreach/reports/sb24-585635 (last visited Jul. 29, 2024); AbbVie Inc., OFFICE OF THE ATTORNEY GENERAL, *Submitted Breach Notification Sample*, OFFICE OF THE ATTORNEY GENERAL, https://oag.ca.gov/ecrime/databreach/reports/sb24-585726 (last visited Jul. 29, 2024); Regeneron Pharmaceuticals, Inc., *Submitted Breach Notification Sample*, OFFICE OF THE ATTORNEY GENERAL, https://oag.ca.gov/ecrime/databreach/reports/sb24-585823 (last visited Jul. 29, 2024); Genentech Inc., *Submitted Breach Notification Sample*, OFFICE OF THE ATTORNEY GENERAL, https://oag.ca.gov/ecrime/databreach/reports/sb24-585650 (last visited Jul. 29, 2024); Incyte Corporation., *Submitted Breach Notification Sample*, OFFICE OF THE ATTORNEY GENERAL, https://oag.ca.gov/ecrime/databreach/reports/sb24-585847 (last visited Jul. 29, 2024); Sumitomo Pharma America, Inc., *Submitted Breach Notification Sample*, OFFICE OF THE ATTORNEY GENERAL, https://oag.ca.gov/ecrime/databreach/reports/sb24-585855 (last visited Jul. 29, 2024); Acadia Pharmaceuticals Inc.,

12. While Cencora initially disclosed the Data Breach in a public filing on February 27, 2024, it revealed very little information.[5] To date, it is still unknown just how many individuals' PII and PHI were implicated as a result of the Data Breach. Additionally, despite becoming aware of unauthorized access to its systems on February 21, 2024, Defendants did not begin notifying affected individuals until late May 2024.

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

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

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

Submitted Breach Notification Sample, OFFICE OF THE ATTORNEY GENERAL, https://oag.ca.gov/ecrime/databreach/reports/sb24-585716 (last visited Jul. 29, 2024); GlaxoSmithKline Group of Companies and the GlaxoSmithKline Patient Access Programs Foundation, *Submitted Breach Notification Sample*, OFFICE OF THE ATTORNEY GENERAL, https://oag.ca.gov/ecrime/databreach/reports/sb24-585929 (last visited Jul. 29, 2024); Endo Pharmaceuticals, Inc., *Submitted Breach Notification Sample*, OFFICE OF THE ATTORNEY GENERAL, https://oag.ca.gov/ecrime/databreach/reports/sb24-585914 (last visited Jul. 29, 2024); Dendreon Pharmaceuticals LLC, *Submitted Breach Notification Sample*, OFFICE OF THE ATTORNEY GENERAL, https://oag.ca.gov/ecrime/databreach/reports/sb24-585889 (last visited Jul. 29, 2024).

[5] Cencora, Inc., Current Report (Form 8-K) (Feb. 21, 2024), https://www.sec.gov/Archives/edgar/data/1140859/000110465924028288/0001104659-24-028288-index.html.

16. Plaintiffs, on behalf of themselves and the Class as defined herein, bring claims for negligence, negligence *per se*, breach of fiduciary duty, breach of implied contract, unjust enrichment, third-party beneficiary claim for breach of contract, and declaratory judgment, seeking actual and putative damages, with attorneys' fees, costs, and expenses, and appropriate injunctive and declaratory relief.

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

PARTIES

18. Plaintiff Michael Coggins is an adult, who at all relevant times, is and was a citizen and resident of Tuckasegee, North Carolina.

19. Plaintiff Elizabeth Fagot is an adult, who at all relevant times, is and was a citizen and resident of Kenner, Louisiana.

20. Plaintiff Bridget Reardon is an adult, who at all relevant times, is and was a citizen and resident of Queens, New York.

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

22. Defendant The Lash Group LLC is a Delaware limited liability company with a principal place of business located at 1 West First Avenue, Conshohocken, Pennsylvania 19428. Upon

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

23. Defendant Bristol Myers Squibb Company is a Delaware corporation with its principal place of business at Route 206 & Province Line Road, Princeton, New Jersey.

24. Defendant Bristol Myers Squibb Patient Assistance Foundation, Inc., is a 501(c)(3) non-profit with its principal place of business at Route 206 & Province Line Road, Princeton, New Jersey.

JURISDICTION AND VENUE

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

26. This Court has personal jurisdiction over Defendants, as Defendants Cencora and Lash Group both maintain their principal place of business in Conshohocken, Pennsylvania, and have engaged in substantial business activities in Pennsylvania, regularly conduct business in Pennsylvania, and have sufficient minimum contacts in Pennsylvania. At all relevant times, all Defendants (including BMS) operate in and direct commerce within this District.

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

FACTUAL BACKGROUND

A. Defendants Collected and Stored Plaintiffs' and Class Members' PII and PHI

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

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

---

[6] Cencora, Inc., Annual Report (Form 10-K) (Nov. 1, 2023), https://investor.amerisourcebergen.com/files/doc_financials/2023/ar/Cencora-FY2023-10-K-Web-Posting.pdf.

[7] *Id.* at 31.

[8] *Id.* at 5.

[9] Zack Whittaker, *US Pharma Giant Cencora Says Americans' Health Information Stolen in Data Breach*, TECHCRUNCH (May 24, 2024), https://techcrunch.com/2024/05/24/cencora-americans-health-data-stolen-breach-cyberattack/.

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

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

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

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

34. BMS is one of many pharmaceutical affiliates that entrusted their patients' PII and PHI with Cencora and Lash Group. Defendant Bristol Myers Squibb Patient Assistance Foundation is an independent charitable organization that provides certain Bristol Myers Squibb medicines to eligible patients free of charge.[12]

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

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

---

[10] *Our Network*, LASH GROUP, https://www.lashgroup.com/our-network (last visited Jul. 29, 2024).

[11] *Who We Are*, CENCORA, https://www.cencora.com/who-we-are (last visited Jul. 29, 2024); *Who We Are*, LASH GROUP, https://www.lashgroup.com/who-we-are (last visited Jul. 29, 2024).

[12] *What is the Bristol Myers Squibb Patient Assistance Foundation*, BRISTOL MYERS SQUIBB PATIENT ASSISTANCE FOUNDATION, https://www.bmspaf.org/#/about (last visited Jul. 29, 2024).

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

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

B. Defendants Are Subject to HIPAA as Business Associates

39. Upon information and belief, Defendants are Health Insurance Portability and Accountability Act ("HIPAA") covered business associates that provide services to various healthcare providers (*i.e.*, HIPAA "Covered Entities").[13]

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

41. Due to their status as HIPAA-covered business associates, Defendants are required to enter into contracts with its Covered Entities to ensure that Defendants will implement adequate safeguards to prevent unauthorized use or disclosure of PHI, including by implementing requirements of the HIPAA Security Rule[14] and to report to the Covered Entities any unauthorized

[13] *See* 45 C.F.R. §160.103.

[14] 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

use or disclosure of PHI, including incidents that constitute breaches of unsecured PHI as in the case of the Data Breach complained of herein.

42. Indeed, both Cencora and Lash Group Defendants claim to maintain protected information in compliance with HIPAA requirements.[15] Likewise, BMS claims to maintain protected information beyond mere compliance with the law.[16]

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

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

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

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

46. These risks are not theoretical; in recent years, numerous high-profile breaches have occurred at business such as Equifax, Facebook, Yahoo, Marriott, Anthem, and other healthcare

---

administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of electronic protected health information. *See* 45 C.F.R. Part 160 and Part 164, Subparts A and C.

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

[16] Privacy Notice Center, BRISTOL MYERS SQUIBB, https://www.bms.com/privacy-policy.html (last visited Jul. 29, 2024).

partner and provider companies, including Managed Care of North America, OneTouchPoint, Inc., Shields Healthcare Group, Eye Care Leaders and Connexin Software, Inc., and Blackbaud.

47. PII has considerable value and constitutes an enticing and well-known target to hackers. Hackers easily can sell stolen data as there has been a "proliferation of open and anonymous cybercrime forums on the Dark Web that serve as a bustling marketplace for such commerce."[17] PHI, in addition to being of a highly personal and private nature, can be used for medical fraud and to submit false medical claims for reimbursement.

48. The prevalence of data breaches and identity theft has increased dramatically in recent years, accompanied by a parallel and growing economic drain on individuals, businesses, and government entities in the United States. In 2021, there were 4,145 publicly disclosed data breaches, exposing 22 billion records. The United States specifically saw a 10% increase in the total number of data breaches.[18]

49. In tandem with the increase in data breaches, the rate of identity theft complaints has also increased over the past few years. For instance, in 2017, 2.9 million people reported some form of identity fraud compared to 5.7 million people in 2021.[19]

50. The healthcare industry has become a prime target for threat actors: "High demand for patient information and often-outdated systems are among the nine reasons healthcare is now the

---

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

[18] *Data Breach Report: 2021 Year End*, RISK BASED SECURITY (Feb. 4, 2022), https://www.riskbasedsecurity.com/2022/02/04/data-breach-report-2021-year-end/.

[19] *Insurance Information Institute, Facts + Statistics: Identity theft and cybercrime*, INSURANCE INFORMATION INSTITUTE, https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime#Identity%20Theft%20And%20Fraud%20Reports,%202015-2019%20 (last visited Jul. 29, 2024).

biggest target for online attacks."[20] Indeed, "[t]he IT environments of healthcare organizations are often complex and difficult to secure. Devices and software continue to be used that have reached end-of-life, as upgrading is costly and often problematic. Many healthcare providers use software solutions that have been developed to work on specific – and now obsolete – operating systems and cannot be transferred to supported operating systems."[21]

51. Cybercriminals seek out PHI at a greater rate than other sources of personal information. Between 2009 and 2022, 5,150 healthcare data breaches of 500 or more individuals have been reported to Health and Human Services' Office of Civil Rights, resulting in the exposure or unauthorized disclosure of the information of 382,262,109 individuals – "[t]hat equates to more than 1.2x the population of the United States."[22]

52. Further, the rate of healthcare data breaches has been on the rise in recent years. "In 2018, healthcare data breaches of 500 or more records were being reported at a rate of around 1 per day. Fast forward 5 years and the rate has more than doubled. In 2022, an average of 1.94 healthcare data breaches of 500 or more records were reported each day."[23]

53. In a 2022 report, the healthcare compliance company Protenus found that there were 905 medical data breaches in 2021, leaving over 50 million patient records exposed for 700 of the 2021 incidents. This is an increase from the 758 medical data breaches that Protenus compiled in 2020.[24]

---

[20] *The healthcare industry is at risk*, SWIVELSECURE, https://swivelsecure.com/solutions/healthcare/healthcare-is-the-biggest-target-for-cyberattacks/ (last visited Jul. 29, 2024).

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

[22] *Healthcare Data Breach Statistics*, HIPAA J., https://www.hipaajournal.com/healthcare-data-breach-statistics/ (last visited Jul. 29, 2024).

[23] *Id.*

[24] *2022 Breach Barometer*, PROTENUS, https://www.protenus.com/breach-barometer-report (last visited Jul. 29, 2024).

54. The healthcare sector suffered about 337 breaches in the first half of 2022 alone, according to Fortified Health Security's mid-year report released in July. The percentage of healthcare breaches attributed to malicious activity rose more than 5 percentage points in the first six months of 2022 to account for nearly 80 percent of all reported incidents.[25]

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

56. Medical Information – As indicated by Jim Trainor, former second in command at the FBI's cyber security division: "Medical records are a gold mine for criminals—they can access a patient's name, DOB, Social Security and insurance numbers, and even financial information all in one place. Credit cards can be, say, five dollars or more where PHI records can go from $20 say up to—we've even seen $60 or $70."[26] A complete identity theft kit that includes health insurance credentials may be worth up to $1,000 on the black market, whereas stolen payment card information sells for about $1.[27]

57. Indeed, medical records "are so valuable because they can be used to commit a multitude of crimes. Healthcare data can be used to impersonate patients to obtain expensive medical services, Medicare and Medicaid benefits, healthcare devices, and prescription medications.

---

[25] Jill McKeon, *Health Sector Suffered 337 Healthcare Data Breaches in First Half of Year*, CYBERSECURITY NEWS (July 19, 2022), https://healthitsecurity.com/news/health-sector-suffered-337-healthcare-data-breaches-in-first-half-of-year.

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

[27] *Managing cyber risks in an interconnected world, Key findings from The Global State of Information Security® Survey 2015*, PRICEWATERHOUSECOOPERS, https://www.pwc.com/gx/en/consulting-services/information-security-survey/assets/the-global-state-of-information-security-survey-2015.pdf (last visited Jul. 29, 2024).

Healthcare records also contain the necessary information to allow fraudulent tax returns to be filed to obtain rebates."[28]

58. "In contrast to credit card numbers and other financial information, healthcare data has an incredibly long lifespan and can often be misused for long periods undetected. Credit card companies monitor for fraud and rapidly block cards and accounts if suspicious activity is detected, but misuse of healthcare data is harder to identify and can be misused in many ways before any malicious activity is detected. During that time, criminals can run up huge debts – far more than is usually possible with stolen credit card information."[29]

59. According to Experian:

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

60. Victims of healthcare data breaches may also find themselves being denied care, coverage, or reimbursement by their medical insurers, having their policies canceled or having to pay to reinstate their insurance, along with suffering damage to their credit ratings and scores. In the worst cases, they've been threatened with losing custody of their children, been charged with drug trafficking, found it hard to get hired for a job, or even been fired by their employers.[30]

61. Even if stolen PII or PHI does not include financial or payment card account information, that does not mean there has been no harm, or that the breach does not cause a substantial risk of identity theft. Freshly stolen information can be used with success against victims in specifically

---

[28] Alder, *supra* note 19.

[29] *Id.*

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

targeted efforts to commit identity theft known as social engineering or spear phishing. In these forms of attack, the criminal uses the previously obtained PII and PHI about the individual, such as name, address, email address, and affiliations, to gain trust and increase the likelihood that a victim will be deceived into providing the criminal with additional information.

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

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

> Information security risks have generally increased in recent years because of the proliferation of cloud-based infrastructure and other services, new technologies, and the increased sophistication and activities of perpetrators of cyberattacks. Security incidents such as ransomware attacks are becoming increasingly prevalent and severe, as well as increasingly difficult to detect. These risks have increased with the growth of our business, including as we integrate the information systems of acquired businesses, such as Alliance Healthcare, into our enterprise.
>
> In addition, security incidents may disrupt our businesses and require that we expend substantial additional resources related to the security of information systems. We, and our third-party service providers, have experienced cyberattacks. For example, in March 2023, one of our foreign business units experienced a cybersecurity event that resulted in the unavailability of certain data stored on a standalone legacy information technology platform and disrupted operations of the Company's foreign business unit in that country. Although the prior incidents did not have a material impact on us, either individually or in the aggregate, similar incidents or events in the future may materially impact our business, reputation, or financial results.
>
> Security breaches can also occur as a result of non-technical issues, including intentional or inadvertent actions by our employees, third-party service providers or their personnel or other parties.[31]

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

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

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

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

> On February 21, 2024, Cencora, Inc. (the "Company"), learned that data from its information systems had been exfiltrated, some of which may contain personal information. Upon initial detection of the unauthorized activity, the Company immediately took containment steps and commenced an investigation with the assistance of law enforcement, cybersecurity experts and external counsel.[32]

66. Approximately three months thereafter, Defendants finally began to send notice letters to affected individuals.[33] The notice letters were sent on Cencora letterhead by some of the largest pharmaceutical firms in the United States, and all attributed the exposure and exfiltration of PII and PHI to the Data Breach.[34]

67. The notice letters, all substantively identical, inform affected individuals that their PII and PHI (including, *inter alia*, consumers' first names, last names, dates of birth, health diagnoses, medications, and prescriptions) had been exfiltrated from Cencora's information systems in the Data Breach.[35]

---

[32] Form 8-K, *supra* note 5.

[33] *See* Submitted Breach Notification Samples, *supra* note 4.

[34] *Id.*; Toulas, *supra* note 1.

[35] *See* Submitted Breach Notification Samples, *supra* note 4.

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

69. Defendants have yet to report the number of individuals affected by the Data Breach. When asked by journalists, a Cencora spokesperson was "unwilling to say if the company has determined how many individuals are affected by the breach and how many individuals the company has notified to date."[36]

70. However, based on Defendants' notifications to state Attorney Generals, the Data Breach at a minimum, has impacted hundreds of thousands of individuals.[37]

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

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

E. Defendants Failed to Comply with FTC Guidelines

73. Defendants are prohibited by the Federal Trade Commission Act, 15 U.S.C. §45 ("FTC Act"), from engaging in "unfair or deceptive acts or practices in or affecting commerce." The Federal Trade Commission ("FTC") has concluded that a company's failure to maintain reasonable

[36] Whittaker, *supra* note 9.

[37] Steve Alder, *More than a Dozen Pharmaceutical Companies Affected by Cencora Cyberattack*, HIPAA J. (May 27, 2024), https://www.hipaajournal.com/cencora-cyberattack-data-breach/.

and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of the FTC Act.

74. The FTC has promulgated numerous guides for businesses that highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[38]

75. In 2016, the FTC updated its publication titled Protecting Personal Information: A Guide for Business, which established cyber-security guidelines for businesses.[39] The guidelines state that:

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

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

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

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

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

76. In another publication, the FTC recommended that companies not maintain PII longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious

[38] *Start with Security: A Guide for Business*, FED. TRADE COMM'N, https://www.ftc.gov/business-guidance/resources/start-security-guide-business (last visited Jul. 29, 2024).

[39] *See 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.

activity on the network; and verify that third-party service providers have implemented reasonable security measures.[40]

77. Notably, the FTC treats the failure to employ reasonable data security safeguards as an unfair act or practice prohibited by Section 5 of the FTC Act. Indeed, the FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the FTC Act. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

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

79. Similarly, the U.S. Government's National Institute of Standards and Technology ("NIST") provides a comprehensive cybersecurity framework that companies of any size can use to evaluate and improve their information security controls.[41]

80. NIST publications include substantive recommendations and procedural guidance pertaining to a broad set of cybersecurity topics including risk assessments, risk management strategies, access controls, training, data security controls, network monitoring, breach detection,

---

[40] *See Start with Security: A Guide for Business*, FED. TRADE COMM'N, (June 2015), https://www.ftc.gov/tips-advice/business-center/guidance/start-security-guide-business.

[41] *See Framework for Improving Critical Infrastructure Cybersecurity*, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (Apr. 16, 2018), Appendix A, Table 2, available at https://nvlpubs.nist.gov/nistpubs/cswp/nist.cswp.04162018.pdf.

and incident response.[42] Upon information and belief, Defendants failed to adhere to the NIST guidance.

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

a) Email protection systems and controls;

b) Endpoint protection systems;

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

d) Data protection and loss prevention measures;

e) IT asset management;

f) Network management;

g) Vulnerability management;

h) Security operations center & incident response; and

i) Cybersecurity oversight and governance policies, procedures, and processes.[43]

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

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

---

42 *Id.* at Table 2 pg. 26-43.

43 *HICP's 10 Mitigating Practices*, HHS, https://405d.hhs.gov/best-practices (last visited Jul. 29, 2024).

F. Defendants Are Obligated Under HIPAA to Safeguard Patient PHI

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

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

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

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

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

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

a. Regulated entities should implement security awareness and training for all workforce members and that the training programs should be ongoing, and evolving to be flexible to educate the workforce on new and current cybersecurity treats and how to respond;

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

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

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

e. Regulated entities should implement strong cyber security practices by requiring strong passwords rules and multifactor identification.[44]

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

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

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

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

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

G. Plaintiffs and Class Members Have Suffered Damages

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

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

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

97. With respect to healthcare breaches, another study found "the majority [70 percent] of data impacted by healthcare breaches could be leveraged by hackers to commit fraud or identity theft."[45]

98. "Actors buying and selling PII and PHI from healthcare institutions and providers in underground marketplaces is very common and will almost certainly remain so due to this data's utility in a wide variety of malicious activity ranging from identity theft and financial fraud to crafting of bespoke phishing lures."[46]

99. Indeed, PII and PHI are valuable commodities to identity thieves and once they have been compromised, criminals will use them and trade the information on the cyber black market for years thereafter. All-inclusive health insurance dossiers containing sensitive health insurance information, names, addresses, telephone numbers, email addresses, Social Security Numbers, and bank account information, complete with account routing numbers can fetch up to $1,200 to $1,300 each on the black market.[47] According to a report released by the FBI's cyber division, criminals

---

[45] Jessica David, *70% of Data Involved in Healthcare Breaches Increases Risk of Fraud*, HEALTHITSECURITY, https://healthitsecurity.com/news/70-of-data-involved-in-healthcare-breaches-increases-risk-of-fraud (last visited July 29, 2024).

[46] *Id*.

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

can sell healthcare records for 50 times the price of stolen Social Security Numbers or credit card numbers.[48]

100. The reality is that cybercriminals seek nefarious outcomes from a data breach and "stolen health data can be used to carry out a variety of crimes."[49]

101. Health information, in particular, is likely to be used in detrimental ways, by leveraging sensitive personal health details and diagnoses to extort or coerce someone, and serious and long-term identity theft.[50]

102. "Medical identity theft is a great concern not only because of its rapid growth rate, but because it is the most expensive and time consuming to resolve of all types of identity theft. Additionally, medical identity theft is very difficult to detect which makes this form of fraud extremely dangerous."[51]

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

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

---

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

[49] Andrew Steger, *What Happens to Stolen Healthcare Data?*, HEALTHTECH, (Oct. 30, 2019), https://healthtechmagazine.net/article/2019/10/what-happens-stolen-healthcare-data-perfcon.

[50] *Id.*

[51] *Consequences of Med. Identity Theft & Healthcare Data Breaches*, EXPERIAN, (Apr. 15, 2010), https://www.experian.com/innovation/thought-leadership/medical-identity-theft-healthcare-data-breaches.jsp

H. Plaintiffs' Experiences and the Data Breach

105. Defendants Cencora and Lash Group were entrusted with Plaintiffs' PII and PHI to facilitate access to their clients' patient support programs. In requesting and maintaining Plaintiffs' PII and PHI, Defendants Cencora and Lash Group undertook a duty to act reasonably in its handling of Plaintiffs' PII and PHI. Defendants Cencora and Lash Group, however, did not take reasonable care of Plaintiffs' PII and PHI, leading to its exposure and compromise as direct and proximate result of Defendants' inadequate data security measures.

106. Further, Defendant BMS was entrusted with Plaintiff Coggins' PII and PHI to facilitate access to their clients' patient support programs. In requesting and maintaining Plaintiff Coggins' PII and PHI, Defendant BMS undertook a duty to act reasonably in its handling of Plaintiff Coggins' PII and PHI. Defendant BMS, however, did not take reasonable care of Plaintiff Coggins' PII and PHI, leading to its exposure and compromise as direct and proximate result of Defendant's inadequate data security measures.

107. Plaintiff Michael Coggins received a Data Breach Notification Letter dated May 17, 2024 from Defendants Cencora and Lash Group informing him that his PII and PHI he directly and/or indirectly provided to Defendants through patient support and access programs managed on behalf of BMS was compromised in the Data Breach. The letter put the onus on Plaintiff Coggins to protect his PII and PHI by encouraging Plaintiff Coggins to remain vigilant.

108. Plaintiff Elizabeth Fagot received a Data Breach Notification Letter dated May 30, 2024 from Defendants Cencora and Lash Group informing her that her PII and PHI she directly and/or indirectly provided to Defendants was compromised in the Data Breach. The letter put the onus on Plaintiff Fagot to protect her PII and PHI by encouraging Plaintiff Fagot to remain vigilant.

109. Plaintiff Bridget Reardon received a Data Breach Notification Letter dated May 28, 2024 from Defendants Cencora and Lash Group informing her that her PII and PHI she directly and/or indirectly provided to Defendants was compromised in the Data Breach. The letter put the onus on Plaintiff Reardon to protect her PII and PHI by encouraging Plaintiff Reardon to remain vigilant.

110. Plaintiffs have suffered actual injury from having their PII and PHI exposed and/or stolen as a result of the Data Breach, including: (a) damages to and diminution of the value of their PII and PHI, a form of intangible property that loses value when it falls into the hands of criminals who are using that information for fraud or publishing the information for sale on the dark web; and (b) loss of privacy.

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

CLASS ACTION ALLEGATIONS

112. Plaintiffs bring this Class Action on behalf of themselves and all other similarly situated individuals pursuant to Rule 23 of the Federal Rules of Civil Procedure.

113. Plaintiffs seek to represent the following Class of persons defined as follows:

> **Nationwide Class:** All persons in the United States and its territories whose PII and/or PHI was compromised as a result of the Data Breach of Cencora's systems reported on February 27, 2024 (the "Class").

114. Plaintiffs also seek certification of the following statewide subclasses, defined as follows and subject to amendment as appropriate:

BMS Subclass: All persons in the United States and its territories whose PII and PHI was provided to BMS or to Cencora at BMS's behest to receive services from BMS and was accessed in the Data Breach by unauthorized persons, including all such persons who were sent a notice of the Data Breach (the "BMS Subclass").

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

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

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

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

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

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

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

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

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

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

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

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

breached their duty to Plaintiffs and Class Members, then Plaintiffs and each Class member suffered damages by that conduct.

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

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

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

125. Plaintiffs restate and reallege the allegations contained in every preceding paragraph as if fully set forth herein.

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

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

128. Defendants' duty to use reasonable care arose from several sources, including but not limited to those described below.

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

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

train and supervise employees and third party vendors with access or credentials to systems and databases containing sensitive PII and PHI.

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

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

a) Theft of their PII and PHI;

b) Costs associated with requesting credit freezes;

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

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

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

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

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

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

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

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

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

134. Plaintiffs restate and reallege the allegations contained in every preceding paragraph as if fully set forth herein.

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

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

137. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce" including, as interpreted and enforced by the FTC, the unfair act or practice by entities such as Defendants or failing to use reasonable measures to protect PII and PHI. Various FTC publications and orders also form the basis of Defendants' duty.

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

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

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

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

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

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

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

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

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

147. As a direct and proximate result of Defendants' negligence *per se*, Plaintiffs and Class Members have suffered injuries, including those identified above in paragraph 131.

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

THIRD CAUSE OF ACTION
BREACH OF FIDUCIARY DUTY

(On Behalf of Plaintiff Coggins and the BMS Subclass as against BMS, and On Behalf of the Class as against Cencora and Lash Group)

149. Plaintiffs restate and reallege the allegations contained in every preceding paragraph as if fully set forth herein.

150. All Plaintiffs bring this claim, individually and on behalf of the Class against Defendants Cencora, Inc. and The Lash Group LLC.

151. Plaintiff Coggins brings this claim, individually and on behalf of the BMS Subclass, against Defendants Bristol Myers Squibb Company and Bristol Myers Squibb Patient Assistance Foundation, Inc.

152. These Plaintiffs and Subclass members gave, directly or indirectly, Cencora and/or BMS their PII and PHI in confidence, believing that Defendants would protect their information. Plaintiffs and Subclass members would not have provided Defendants with this information had they known it would not be adequately protected.

153. Defendants' acceptance and storage of Plaintiffs' and Class members' PII and PHI created a fiduciary relationship between the Defendants and their respective Plaintiffs and BMS Subclass members. In light of this relationship, the Defendants must act primarily for the benefit of their current and former patients or customers, which includes safeguarding and protecting Plaintiffs' and Subclass members' PII and PHI.

154. Defendants had a fiduciary duty to act for the benefit of Plaintiffs and Subclass members upon matters within the scope of their relationship. Defendants breached that duty by failing to, or

contracting with companies that failed to, properly protect the integrity of the system(s) containing Plaintiffs' and Subclass members' PII and PHI, failing to comply with the data security guidelines set forth by HIPAA, and otherwise failing to safeguard Plaintiffs' and Subclass members' PII and PHI that it collected and maintained.

155. As a direct and proximate result of Defendants' breaches of their fiduciary duties, Plaintiffs and Subclass members have suffered and will suffer injury, including, but not limited to: (i) a substantial increase in the likelihood of, or imminent threat of, identity theft; (ii) the compromise, publication, and theft of their Private Information; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from unauthorized use of their PII and PHI; (iv) lost opportunity costs associated with effort attempting to mitigate the actual and future consequences of the Data Breach; (v) the continued risk to their PII and PHI which remains in Defendants' possession; (vi) future costs in terms of time, effort, and money that will be required to prevent, detect, and repair the impact of the PII and PHI compromised as a result of the Data Breach; and (vii) overpayment for the services that were received without adequate data security.

FOURTH CAUSE OF ACTION
BREACH OF IMPLIED CONTRACT

(On Behalf of Plaintiff Coggins and the BMS Subclass as against BMS, and On Behalf of the Class as against Cencora and Lash Group)

156. Plaintiffs restate and reallege the allegations contained in every preceding paragraph as if fully set forth herein.

157. All Plaintiffs bring this claim, individually and on behalf of the Class against Defendants Cencora, Inc., and The Lash Group LLC.

158. Plaintiff Coggins brings this claim, individually and on behalf of the BMS Subclass against Defendants Bristol Myers Squibb Company and Bristol Myers Squibb Patient Assistance Foundation, Inc.

159. In connection with receiving medications or medical services, Plaintiffs and Subclass members entered into implied contracts with Defendants.

160. Pursuant to these implied contracts, Plaintiffs and Subclass members paid money, whether directly, or through their insurers (and/or pharmacies), and provided Defendants with their PII and PHI. In exchange, affiliate partners agreed to, and Plaintiffs and Subclass members understood that, affiliate partners would, among other things: (1) provide medications or medical services to Plaintiffs and Subclass members; (2) take reasonable measures to protect the security and confidentiality of Plaintiffs' and Subclass members' PII and PHI; and (3) protect Plaintiffs' and Subclass members' PII and PHI in compliance with federal and state laws and regulations and industry standards.

161. The protection of PII and PHI was a material term under the implied contracts between Plaintiffs and Subclass members, on one hand, and the Defendants on the other hand. Had Plaintiffs and Class members known that Defendants would not adequately protect their current and former customers' PII and PHI, they would not have sought healthcare services from affiliate partners.

162. Plaintiffs and Subclass members performed their obligations under the implied contract when they provided Defendants with their PII and PHI and paid – directly or indirectly – for medications, health care, or other services.

163. Defendants breached their obligations under their implied contracts with Plaintiffs and Subclass members in failing to implement and maintain reasonable security measures to protect and secure their PII and PHI and in failing to implement and maintain security protocols and procedures to protect Plaintiffs' and Subclass members' PII and PHI in a manner that complies with applicable laws, regulations, and industry standards.

164. Defendants' breach of their obligations under their implied contracts with Plaintiffs and Subclass members directly resulted in the Data Breach and the injuries that Plaintiffs and Subclass members have suffered from the Data Breach.

165. Plaintiffs and all other Subclass members were damaged by Defendants' breach of implied contracts because: (i) they paid – directly or indirectly – for data security protection they did not receive; (ii) they face a substantially increased risk or imminent threat of identity theft and medical identity theft – risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (iii) their PII and PHI was improperly disclosed to unauthorized individuals; (iv) the confidentiality of their PII and PHI has been breached; (v) they were deprived of the value of their PII and PHI, for which there is a well-established national and international market; (vi) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of medical identity theft they face and will continue to face; and (vii) overpayment for the services that were received without adequate data security.

FIFTH CAUSE OF ACTION
UNJUST ENRICHMENT
(On Behalf of Plaintiffs and the Class Against All Defendants)

166. Plaintiffs restate and reallege the allegations contained in every preceding paragraph as if fully set forth herein.

167. Additionally, or in the alternative, Plaintiffs and the Class bring this claim for unjust enrichment.

168. 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 PII and PHI. 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 PII and PHI protected with adequate data security.

169. Defendants knew that Plaintiffs and Class members conferred a benefit upon it and had accepted and retained that benefit by accepting and retaining the PII and PHI entrusted to it. Defendants profited from Plaintiffs' and Class members' retained data and used Plaintiffs' and Class members' PII and PHI for business purposes.

170. Defendants failed to secure Plaintiffs' and Class members' PII and PHI and, therefore, did not fully compensate Plaintiffs or Class members for the value that PII and PHI provided.

171. Defendants acquired the PII and PHI through inequitable record retention, having failed to investigate and/or disclose the inadequate data security practices previously mentioned.

172. 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 PII and PHI, they would not have entrusted their PII and PHI to Defendants or obtained services from Defendants.

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

174. Defendants enriched themselves by saving the costs they reasonably should have expended on data security measures to secure Plaintiffs' and Class members' PII and PHI. 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.

175. 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 PII and PHI.

176. 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.

177. As a direct and proximate result of Defendants' conduct, Plaintiffs and Class members have suffered and will suffer injury, including: (i) invasion of privacy; (ii) theft of their PII and PHI; (iii) lost or diminished value of PII and PHI; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) statutory damages; (viii) nominal damages; and (ix) the continued and certainly increased risk to their PII and PHI, 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 PII and PHI.

178. 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.

179. 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.

SIXTH CAUSE OF ACTION
THIRD-PARTY BENEFICIARY CLAIM FOR BREACH OF CONTRACT
(On Behalf of Plaintiffs and the Class Against Cencora and Lash Group)

180. Plaintiffs restate and reallege the allegations contained in every preceding paragraph as if fully set forth herein.

181. Defendants Cencora and Lash Group entered into a contract to provide services to Plaintiffs' and Class members' pharmacies, pharmaceutical companies, healthcare providers, or patient support programs. Upon information and belief, this contract is virtually identical to the contracts entered into between Cencora and Lash Group and their other medical or pharmacy provider customers around the country whose patients were also affected by the Data Breach.

182. These contracts were made expressly for the benefit of Plaintiffs and the Class, as it was their confidential medical information that Cencora and Lash Group agreed to collect and protect through their services. Thus, the benefit of collection and protection of the PII and PHI belonging to Plaintiffs and the Class was the direct and primary objective of the contracting parties.

183. Cencora and Lash Group knew that if they were to breach these contracts with their customers, the customers' patients, including Plaintiffs and the Class, would be harmed by, among other harms, fraudulent transactions.

184. Cencora and Lash Group breached their contracts with Plaintiffs' and Class Members' pharmacies, pharmaceutical companies, healthcare providers, or patient support programs affected by this Data Breach when they failed to use reasonable data security measures that could have prevented the Data Breach.

185. As foreseen, Plaintiffs and the Class were harmed by Cencora's and Lash Group's failure to use reasonable security measures to store patient information, including but not limited to the risk of harm through the loss of their PII and PHI, increased out-of-pocket medical expenses, and loss of access to medications and/or healthcare treatment and other services.

186. Accordingly, Plaintiffs and the Class are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

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

187. Plaintiffs restate and reallege the allegations contained in every preceding paragraph as if fully set forth herein.

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

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

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

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

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

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

192. 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 of any of Defendants' systems. The risk of another such breach is real, immediate, and substantial. If another breach of any of Defendants' systems occurs, 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.

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

194. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach of Defendants' systems, thus eliminating the additional injuries that would result to Plaintiffs, Class Members, and patients whose confidential information would be further compromised.

DEMAND FOR JURY TRIAL

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

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and all others similarly situated, pray for relief as follows:

1. Certifying the Class under Rule 23 of the Federal Rules of Civil Procedure and naming Plaintiffs as representatives of the Class and Plaintiffs' attorneys as Class Counsel to represent the Class;

2. Ruling in favor of Plaintiffs and the Class on all counts asserted herein;

3. Awarding compensatory damages on behalf of Plaintiffs and the Class;

4. Awarding punitive damages on behalf of Plaintiffs and the Class;

5. Awarding restitution, disgorgement, and all other forms of equitable monetary relief described herein;

6. Awarding Declaratory and injunctive relief as described herein;

7. Awarding Plaintiffs reasonable attorneys' fees, costs, and expenses;

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

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

10. Granting all other and further relief as this Court deems just and proper.

Dated: July 31, 2024

Respectfully submitted,

/s/ Charles E. Schaffer
Charles E. Schaffer
LEVIN SEDRAN & BERMAN LLP
510 Walnut Street, Ste. 500
Philadelphia, PA 19106
Telephone: (215) 592-1500
Facsimile: (215) 592-4663
cshaffer@lfsblaw.com

/s/ Joseph P. Guglielmo
Joseph P. Guglielmo
Amanda M. Rolon
SCOTT+SCOTT ATTORNEYS AT LAW LLP
The Helmsley Building
230 Park Avenue, 17th Fl.
New York, NY 10169
Telephone: (212) 223-6444
Facsimile: (212) 223-6334
jguglielmo@scott-scott.com
arolon@scott-scott.com