

UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF PENNSYLVANIA

MARILYN BORNE and CELIA SKORUPSKI, *individually and on behalf of all others similarly situated,*

Plaintiffs,

v.

CENCORA, INC., THE LASH GROUP, LLC, BRISTOL-MEYERS SQUIBB COMPANY, and BRISTOL-MEYERS SQUIBB PATIENT ASSISTANCE FOUNDATION, INC.,

Defendants.

Case No.

CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

Plaintiffs Marilyn Borne and Celia Skorupski (“Plaintiffs”) bring this Class Action Complaint, individually and on behalf of all others similarly situated (the “Class Members”), against Defendants Cencora, Inc. (“Cencora”), The Lash Group, LLC (“Lash Group”), Bristol-Myers Squibb Company and Bristol- Meyers Squibb Patient Assistance Foundation, Inc. (together, “BMS” and collectively with “Cencora” and “Lash Group,” “Defendants”), and allege as follows, based upon information and belief, investigation of counsel, and the personal knowledge of Plaintiffs.

NATURE OF CASE

1. This class action arises out of the recent targeted cyberattack and data breach where unauthorized third-party criminals retrieved and exfiltrated the highly sensitive data of Plaintiffs and hundreds of millions of Class Members, as a result of Defendants’ failure to reasonably and adequately secure this highly-sensitive consumer data (the “Data Breach”). The Data Breach was the result of a “smash-and-grab” attack, not ransomware.

2. During the regular course of conducting their daily business, Defendants acquire, collect, store, and transfer patients' sensitive personal data, including personally identifying information ("PII") and protected health information ("PHI") (collectively, "Private Information"). More specifically, Defendants Cencora and Lash Group acquired Plaintiffs' and other Class Members' Private Information through the patient support and access programs they manage on behalf of BMS and other pharmacy or pharmaceutical partners. Plaintiffs and Class Members are patients who have no choice other than to provide their sensitive Private Information to Defendants directly or indirectly if they wish to receive medications or to access a pharmacy benefit program.

3. Defendants Cencora and Lash Group partner with pharmaceutical companies, pharmacies, and healthcare providers to facilitate access to therapies through drug distribution, patient support services, business analytics and technology, and other services.¹

4. On February 21, 2024, Cencora learned that "data from its systems had been exfiltrated, some of which could contain personal information."² At that time, Cencora filed a brief Form 8-K with the SEC disclosing the attack but did not indicate the attack would compromise the Private Information of patients and consumers entrusted to Cencora by its pharmaceutical partners. Nor did Cencora begin sending notices out to affected individuals until late May.

5. In addition to BMS, at least eleven pharmaceutical firms, each entrusted with the sensitive Private Information of millions of Americans, were impacted by the Data Breach. These firms include Novartis Pharmaceuticals Corporation, Bayer Corporation, AbbVie Inc., Regeneron Pharmaceuticals, Inc., Genentech, Inc., Incyte Corporation, Sumitomo Pharma America, Inc.,

¹ Plaintiff Borne's Data Breach Notice, attached as Exhibit A; Plaintiff Skorupski's Data Breach Notice, attached as Exhibit B.

² Plaintiff Borne's Data Breach Notice, attached as Exhibit A; Plaintiff Skorupski's Data Breach Notice, attached as Exhibit B.

Acadia Pharmaceuticals Inc., GlaxoSmithKline Group, Endo Pharmaceuticals Inc., and Dendreon Pharmaceuticals LLC.³

6. The Private Information compromised in the Data Breach included at least Plaintiffs' and Class Members' first name, last name, address, date of birth, health diagnosis, and/or medications and prescriptions.

7. As of May 28, 2024 at least 500,000 affected individuals had been notified, but the actual number of victims could be much higher considering that Cencora and Lash Group have serviced over 18 million customers to date.⁴

8. Defendants are subject to HIPAA's privacy rules as healthcare business associates because they knowingly obtain, collect, and store patient Private Information. Defendants, therefore, have a duty to secure, maintain, protect, and safeguard the Private Information in their possession against unauthorized access and disclosure through reasonable and adequate data security measures. In light of dozens of recent cyberattacks targeting the healthcare industry and exfiltrating highly sensitive healthcare information and resulting ransoms, at the time of the Data Breach, Defendants were well-aware that Private Information is extremely valuable to cybercriminals. This made it highly foreseeable that Defendants would be the target of a cyberattack.

9. Despite their duties under the law to Plaintiffs and Class Members to protect and safeguard their Private Information, and the foreseeability of a data breach, Defendants failed to implement reasonable and adequate data security measures, which directly resulted in a Data

³ Bill Toulas, *Cencora data breach exposes US patient info from 11 drug companies*, BleepingComputer (May 24, 2024) <https://www.bleepingcomputer.com/news/security/cencora-data-breach-exposes-us-patient-info-from-11-drug-companies/>.

⁴ Krishi Chowdhary, Major Pharmaceutical Companies Hit by Data Breach Linked to Cencora Cyberattack, TechReport (May 28, 2024), <https://techreport.com/news/major-pharmaceutical-companies-data-breach-cencora-cyberattack/>

Breach.

10. 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.

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

12. Now armed with the Private Information accessed in the Data Breach, cybercriminals can use or sell the Private Information to further harm Plaintiffs and Class Members in a variety of ways including: destroying their credit by opening new financial accounts and taking out loans in Class Members' names; using Class Members' names to improperly obtain medical services; using Class Members' Private Information to target other phishing and hacking intrusions; using Class Members' Private Information to obtain government benefits; and otherwise assuming Class Members' identities.

13. As a result of the Data Breach, Plaintiffs and Class Members face a substantial risk of imminent 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.

14. Plaintiffs and Class Members have incurred, and will continue to incur, damages in the form of, among other things, identity theft, attempted identity theft, lost time and expenses

mitigating harms, increased risk of harm, damaged credit, diminished value of Private Information, loss of privacy, and/or additional damages as described below.

15. Accordingly, Plaintiffs bring this action against Defendants, seeking redress for Defendants' unlawful conduct and asserting claims for: (i) negligence; (ii) negligence *per se*; (iii) breach of implied contract; (iv) breach of contractual duties owed to third-party beneficiaries; (v) unjust enrichment; (vi) bailment; and (vii) breach of fiduciary duty.

16. Through these claims, Plaintiffs seek damages in an amount to be proven at trial, as well as injunctive and other equitable relief, including reasonable and adequate improvements to Defendants' data security systems, policies, and practices, the implementation of annual audits reviewing the same, adequate credit monitoring services funded by Defendants, and payment for the costs of repairing damaged credit as a result of the Data Breach.

THE PARTIES

17. Plaintiff Marilyn Borne is a natural person, resident, and citizen of the State of Louisiana.

18. Plaintiff Celia Skorupski is a natural person, resident, and citizen of the state of Connecticut.

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

20. Defendant Lash Group is a part of Defendant Cencora and has its principal place of business at 1 West First Avenue, Conshohocken, Pennsylvania.

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

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

JURISDICTION AND VENUE

23. This Court has original jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2) because Plaintiffs, and at least one member of the putative Class, as defined below, are citizens of a different state than Defendants, there are more than 100 putative class members, and the amount in controversy exceeds \$5 million exclusive of interest and costs.

24. This Court has general personal jurisdiction over Defendants because Defendants Cencora and Lash Group have their principal places of business in this district, and all Defendants operate in and direct commerce at this District.

25. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(b) because Defendants Cencora and Lash Group's principal places of business are located in this District, a substantial part of the events giving rise to this action occurred in this District, and Defendants have harmed Class Members residing in this District.

DEFENDANTS' BUSINESSES

26. Defendant Cencora is a leading pharmaceutical solutions organization which provides "end-to-end pharmaceutical commercialization solutions" and claims to "empower[] patient-centered care all over the world."⁵

27. Defendant Lash Group is a part of Cencora (formerly AmerisourceBergen) with expertise in over 20 therapeutic areas, and which operates over 100 patient support programs.⁶

⁵ Cencora, Who We Are, <https://www.cencora.com/who-we-are> (last visited May 29, 2024).

⁶ AmerisourceBergen: Lash Group, Who We Are, <https://www.lashgroup.com/who-we-are> (last visited May 29, 2024).

28. Defendant Bristol-Meyers Squibb Company is “a global biopharmaceutical company whose mission is to discover, develop and deliver innovative medicines that help patients prevail over serious diseases.”⁷

29. Defendant Bristol-Meyers Squibb Patient Assistance Foundation is an independent charitable organization that provides certain Bristol Meyers Squibb medicines to eligible patients free of charge.⁸

30. Plaintiffs and Class Members are former or current patients and consumers who used Defendants’ services, either directly or indirectly. Plaintiffs and Class Members indirectly used Defendant Cencora’s or Defendant Lash Group’s services when Plaintiffs’ and Class Members’ pharmacies, pharmaceutical companies, healthcare providers, or pharmacy benefit programs (like BMS) contracted with Defendants Cencora and/or Lash Group for their services.

31. In the course of facilitating support to pharmacies, pharmaceutical companies, and healthcare providers related to Plaintiffs’ and Class Members’ healthcare, Defendants receive, create, handle, and transfer patients’ Private Information. Indeed, to receive services from Defendants, either directly or indirectly, Plaintiffs and Class Members were required to provide highly sensitive Private Information, including some or all of the following:

- Full names and addresses;
- Personal email addresses and phone numbers;
- Dates of Birth;
- Social Security numbers;
- Driver’s licenses (or other similar state identifications);

⁷ About Us, Bristol Meyers Squibb, <https://www.bms.com/about-us.html> (last visited May 29, 2024).

⁸ What is the Bristol Meyers Squibb Patient Assistance Foundation, Bristol Meyers Squibb Patient Assistance Foundation, <https://www.bmsspaf.org/#/about> (last visited May 29, 2024).

- Health insurance information;
- Health information including but not limited to information about diagnosis and treatment, personal medical history, family medical history, mental health information, information related to STDs and treatment, information related to abortions, medication information, and medical record numbers;
- Information about physicians and related medical professionals who had been involved in previous or ongoing treatment of the patient;
- Billing and claims information, including but not limited to information related to credit and debit card numbers, bank account statements and account numbers, and insurance payment details;
- Medicare/Medicaid information;
- Medication information; and
- Diagnostic results and treatment information.

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

33. Because of the highly sensitive and personal nature of the information Defendants acquire, store, and transfer with respect to consumers and other individuals, upon information and belief, Defendants promise to, among other things: keep Private Information private; comply with healthcare industry standards related to data security and Private Information, including FTC guidelines; inform consumers of their legal duties and comply with all federal and state laws protecting consumer Private Information; only use and release Private Information for reasons that relate to the products and services Plaintiffs and Class Members obtain from Defendants and provide adequate notice to individuals if their Private Information is disclosed without

authorization.

34. As HIPAA covered business entities, as discussed *infra*, Defendants are required to implement adequate safeguards to prevent unauthorized use or disclosure of Private Information, including by implementing the requirements of the HIPAA Security Rule and to report any unauthorized use or disclosure of Private Information, including incidents that constitute breaches of unsecured PHI, as in the case of the Data Breach complained of herein.

35. However, despite the existence of these duties, Defendants did not maintain adequate security to protect their systems from infiltration by cybercriminals.

36. By obtaining, collecting, using, and deriving a benefit from Plaintiffs' and Class Members' Private Information, Defendants assumed legal and equitable duties owed to Plaintiffs and Class Members and knew or should have known that they were responsible for protecting Plaintiffs' and Class Members' Private Information from unauthorized disclosure.

37. Yet, contrary to Defendants' representations, Defendants failed to implement adequate data security measures, as evidenced by Defendants' admission of the Data Breach, which affected, by some estimates, one-third of all Americans.⁹

Defendants are Covered Entities Subject to HIPAA

38. Defendants are "business associates" of healthcare providers and covered entities under HIPAA, each of whom provide healthcare, medication, pharmacy, and pharmaceutical related services to hundreds of millions of patients annually either directly or via their healthcare clients. As a regular and necessary part of their businesses, Defendants collect, store, and transfer the highly sensitive Private Information of patients.

⁹ Testimony of Andrew Witty Chief during the U.S. Senate Committee on Finance, Hacking America's Health Care: Assessing the Change Healthcare Cyber Attack and What's Next (May 1, 2024).

39. 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.

40. Due to the nature of Defendants' businesses, which includes providing a range of drug distribution, patient support services, business analytics and technology, and other services to healthcare clients, including obtaining, storing, and maintaining electronic health and medical records, Defendants would be unable to engage in their regular business activities without collecting and aggregating Private Information they know and understand to be sensitive and confidential.

41. In fact, whenever Defendants contract with covered entities (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 Rule¹⁰ and immediately reporting any unauthorized use or disclosure of PHI (such as the Data Breach) to affected covered entities.

42. 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.¹¹

¹⁰ The HIPAA Security Rule establishes national standards to protect individuals' electronic personal health information that is created, received, used, or maintained by a covered entity. The Security Rule requires appropriate administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of electronic protected health information. See 45 C.F.R. Part 160 and Part 164, Subparts A and C.

¹¹ Privacy Statement Overview, Cencora, <https://www.cencora.com/global-privacy-statement-overview> (last accessed May 29, 2024) (emphasis added).

43. BMS likewise claims that “your privacy matters to us” and that it adopts “reasonable and appropriate security measures,” stating:

For us, data privacy goes beyond mere compliance with the law. BMS aims to collect, use, and share information that we obtain about you in a manner consistent with our company values, including high ethical standards, integrity, inclusion, fairness, and transparency. We have a dedicated internal team that reviews how BMS accesses, collects, uses, shares, stores, transfers, deletes and protects information about you. To safeguard your data, *BMS employs reasonable and appropriate security measures.*¹²

44. By obtaining, collecting, using, and deriving a benefit from Plaintiffs’ and Class Members’ Private Information, Defendants assumed legal and equitable duties and knew or should have known that they were responsible for protecting Plaintiffs’ and Class Members’ Private Information from unauthorized disclosure.

45. Plaintiffs and Class Members are or were patients, or executors or surviving spouses of patients, whose Private Information was maintained by Defendants and directly or indirectly entrusted Defendants with their Private Information.

46. Plaintiffs and Class Members relied on Defendants to implement and follow adequate data security policies and protocols, to keep their Private Information confidential and securely maintained, to use such Private Information solely for business and healthcare purposes, and to prevent unauthorized disclosures of Private Information. Plaintiffs and Class Members reasonably expected that Defendants would safeguard and keep their Private Information confidential.

47. As described throughout this Complaint, Defendants failed to reasonably and adequately protect, secure, and/or store Plaintiffs’ and Class Members’ Private Information prior to, during, or after the Data Breach, but rather, enacted unreasonable data security measures they

¹² BMS General Privacy Notice, Bristol Meyers Squibb, <https://www.bms.com/assets/bms/us/en-us/pdf/general-privacy-notice.pdf> (last accessed May 29, 2024) (emphasis added).

knew or should have known were insufficient to reasonably protect the highly sensitive Private Information that they maintained. Consequently, cybercriminals circumvented Defendants' security measures, resulting in a significant Data Breach.

The Data Breach of Defendants' Systems

48. Beginning on or around February 21, 2024, Defendant Cencora was subjected to a "smash-and-grab" cyberattack which compromised the sensitive Private Information of Plaintiffs and Class Members. Unlike ransomware attacks, smash-and-grab attacks are characterized by their rapid execution, which make them difficult to detect and halt in real time.¹³

49. In a Form 8-K filed with the SEC, Cencora noted that it learned "that data from its information systems had been exfiltrated, some of which may contain personal information."¹⁴ Cencora's SEC notice also stated that Cencora was investigating the Data Breach:

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.¹⁵

50. Cencora's investigation concluded April 10, 2024, and determined that Plaintiffs' and Class Members' Private Information was compromised in the Data Breach. Specifically, Cencora's investigation discovered that personal information including Plaintiffs' and Class Members' full names, addresses, dates of birth, health diagnoses, and/or medications and prescriptions were exfiltrated in the Data Breach.

51. Yet, Cencora waited over *one month* after determining that Plaintiffs' and Class Member's Private Information was compromised, and over *three months* after it initially

¹³ Sreenu Pasunuri, Digital Heists: The Rising Threat of Smash & Grab Cyber Attacks, LinkedIn (May 20, 2024)<https://www.linkedin.com/pulse/digital-heists-rising-threat-smash-grab-cyber-attacks-sreenu-pasunuri-fhz0c/>.

¹⁴ Cencora, Inc. Form 8-K, U.S. Securities and Exchange Commission (Feb. 21, 2024), https://www.sec.gov/Archives/edgar/data/1140859/000110465924028288/tm247267d1_8k.htm.

¹⁵ *Id.*

discovered the Data Breach to begin notifying affected individuals. Plaintiff Borne still has yet to receive any notice or acknowledgement of the Data Breach from the BMS Defendants to which she entrusted her Private Information in the first instance. Plaintiff Skorupski still has yet to receive notice from the pharmacy benefit program in which she entrusted her Private Information in the first instance.

52. In late May, Cencora sent Plaintiffs and other Class Members a Data Breach Notice which said the following:

What Happened?

On February 21, 2024 Cencora learned that data from its information systems had been exfiltrated, some of which could contain personal information. Upon initial detection of the unauthorized activity, Cencora immediately took containment steps and commenced an investigation with the assistance of law enforcement, cybersecurity experts, and outside lawyers. On April 10, 2024, we confirmed that some of your personal information was affected by the incident.

53. Omitted from the Data Breach Notice is information explaining the root cause of the Data Breach, the vulnerabilities exploited by the cybercriminals, any Defendants' prior data breach histories, and any new remedial measures undertaken to ensure similar breaches do not continue to occur exposing customers' Private Information. To date, these omitted details have not been explained or revealed to Plaintiffs and Class Members, who retain a vested interest in ensuring that their Private Information is not repeatedly exposed to cybercriminals by Defendants.

54. Upon information and belief, the cybercriminals responsible for the Data Breach specifically targeted Defendants based on their status as healthcare entities with enormous amounts of valuable Private Information—including the Private Information of Plaintiffs and Class Members.

55. Plaintiffs further believe that their and Class Members' Private Information has been or soon will be disseminated on the dark web, to be available for purchase, because that is

the *modus operandi* of cybercriminals.

56. As HIPAA covered business entities that collect, create, transfer, and maintain significant volumes of Private Information, the targeted attack was a foreseeable risk which Defendants were aware of, had previously and recently been affected by, and knew they had a duty to guard against. It is well-known that healthcare providers and their business associates, such as Defendants, which collect and store confidential and sensitive Private Information of millions of individuals, are frequently targeted by cyberattacks. Further, cyberattacks are highly preventable through the implementation of reasonable and adequate cybersecurity safeguards, including proper employee cybersecurity training.

57. The U.S. Department of Health and Human Services (“HHS”) and the Office of Consumer Rights urges HIPAA entities to encrypt data containing sensitive personal information. In an effort to underscore the necessity of doing so to protect consumers’ data, as far back as 2014, the Department fined two healthcare companies approximately two million dollars for failing to encrypt laptops containing sensitive personal information. In announcing the fines, Susan McAndrew, formerly OCR’s deputy director of health information privacy, stated that “[o]ur message to these organizations is simple: *encryption is your best defense against these incidents.*” Despite these fines and warnings, Defendants failed to encrypt Plaintiffs’ and Class Members’ Private Information.

58. The Data Breach was a targeted cyberattack expressly designed to gain access to and exfiltrate private and confidential data, including (among other things) the Private Information of patients, like Plaintiffs and Class Members.

59. Defendants had obligations created by HIPAA, contract, industry standards, and common law to keep their Private Information confidential and protected from unauthorized

access and disclosure.

60. Plaintiffs and Class Members (or their healthcare providers, pharmacies, or patient support programs) entrusted Defendants with their Private Information with the reasonable expectation and mutual understanding that Defendants would comply with their obligations to keep such information confidential and secure from unauthorized access.

61. By obtaining, collecting, using, and deriving a benefit from Plaintiffs' and Class Members' Private Information, Defendants assumed legal and equitable duties and knew, or should have known, they were responsible for protecting Plaintiffs' and Class Members' Private Information from unauthorized disclosure.

62. Due to Defendants' inadequate security measures and their delayed notice to victims, Plaintiffs and Class Members were unable to obtain necessary health services and prescriptions affecting their health and wellbeing and now also face a present, immediate, and ongoing risk of fraud and identity theft that they will have to deal with for the rest of their lives.

The Data Breach was a Foreseeable Risk of which Defendants Were on Notice

63. As HIPAA-covered entities handling Private Information, Defendants' data security obligations were particularly important given the substantial increase in cyberattacks and data breaches in the healthcare industry and other industries holding significant amounts of PII and PHI preceding the Data Breach.

64. At all relevant times, Defendants knew, or should have known that Plaintiffs' and Class Members' Private Information was a target for malicious actors. Yet, Defendants failed to implement and maintain reasonable and appropriate data privacy and security measures to protect Plaintiffs' and Class Members' Private Information from cyberattacks that Defendants knew directly about and should have guarded against.

65. The healthcare sector suffered at least 337 data breaches in the first half of 2022 alone, according to Fortified Health Security’s mid-year report released in July 2022. The percentage of healthcare data breaches attributed to malicious activity rose more than five percentage points in the first six months of 2022 to account for nearly 80 percent of all reported incidents.¹⁶

66. 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 (8.8 patients, March 2023), Shields Health Care Group (2 million patients, March 2022), Broward Health (1.3 million patients, January 2022), OneTouchPoint (2.6 million patients, July 2022), Trinity Health (3.3 million patients, May 2020), and American Medical Collection Agency (25 million patients, March 2019)—Defendants knew or should have known their electronic records would be targeted by cybercriminals.

67. PHI is particularly valuable and has been referred to as a “treasure trove for criminals.”¹⁷ A cybercriminal who steals a person’s PHI can end up with as many as “seven to 10 personal identifying characteristics of an individual.”¹⁸ A study by Experian found that the “average total cost” of medical identity theft to the victims of such theft was “about \$20,000” per victim, per incident in 2010, and that a majority of victims of medical identity theft were forced to pay out-of-pocket costs for healthcare they did not receive in order to restore coverage.¹⁹

¹⁶ See Jill McKeon, *Health Sector Suffered 337 Healthcare Data Breaches in First Half of Year*, HEALTH IT SECURITY: CYBERSECURITY NEWS (July 19, 2022), <https://healthitsecurity.com/news/health-sector-suffered-337-healthcare-data-breaches-in-first-half-of-year>.

¹⁷ See Andrew Steger, *What Happens to Stolen Healthcare Data?*, HEALTHTECH MAGAZINE (Oct. 30, 2019), <https://healthtechmagazine.net/article/2019/10/what-happens-stolen-healthcare-data-perfcon> (quoting Tom Kellermann, Chief Cybersecurity Officer, Carbon Black, stating “Health information is a treasure trove for criminals.”).

¹⁸ *Id.*

¹⁹ Elinor Mills, *Study: Medical identity theft is costly for victims*, CNET (Mar. 3, 2010), <https://www.cnet.com/news/privacy/study-medical-identity-theft-is-costly-for-victims/>.

68. In fact, according to the cybersecurity firm Mimecast, 90 percent of healthcare organizations experienced cyberattacks in 2020.²⁰

69. Cyberattacks on medical systems have become so common that in 2019 the FBI and U.S. Secret Service issued a warning to potential targets, so they are aware of, and prepared for, a potential attack. As one report explained, “[e]ntities like smaller municipalities and hospitals are attractive . . . because they often have lesser IT defenses and a high incentive to regain access to their data quickly.”²¹

70. This was not the FBI’s first warning to the healthcare industry about the threat of cyberattacks. Indeed, cyberattacks against the healthcare industry have been common for over a decade, with the FBI warning as early as 2011 that cybercriminals 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[.]” The FBI further warned that “the increasing sophistication of cyber criminals will no doubt lead to an escalation in cybercrime.”²² Later, in August 2014, after a cyberattack on Community Health Systems, Inc., the FBI warned companies within the healthcare industry that hackers were targeting them. The warning stated that “[t]he FBI has observed malicious actors targeting healthcare related systems, perhaps for the purpose of obtaining the Protected Healthcare Information (PHI) and/or Personally Identifiable Information (PII).”

71. According to an article in the HIPAA Journal posted on November 2, 2023, cybercriminals hack into medical practices for their highly prized medical records. “[T]he number of data breaches reported by HIPAA-regulated entities continues to increase every year. 2021 saw

²⁰ See Maria Henriquez, *Iowa City Hospital Suffers Phishing Attack*, SECURITY MAGAZINE (Nov. 23, 2020), <https://www.securitymagazine.com/articles/93988-iowa-city-hospital-suffers-phishing-attack>.

²¹ FBI, *Secret Service Warn of Targeted Ransomware*, LAW360 (Nov. 18, 2019), <https://www.law360.com/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware>.

²² Gordon M. Snow, *Statement before the House Financial Services Committee, Subcommittee on Financial Institutions and Consumer Credit*, FBI (Sept. 14, 2011), <https://archives.fbi.gov/archives/news/testimony/cyber-security-threats-to-the-financial-sector>.

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.”²³

72. According to the HIPAA Journal’s 2023 Healthcare Data Breach Report, “[a]n unwanted record was set in 2023 with 725 large security breaches in healthcare reported to the Department of Health and Human Services Office for Civil Rights, beating the record of 720 healthcare security breaches set the previous year.”²⁴

73. Healthcare organizations are easy targets because “even relatively small healthcare providers may store the records of hundreds of thousands of patients. The stored data is highly detailed, including demographic data, Social Security numbers, financial information, health insurance information, and medical and clinical data, and that information can be easily monetized.”²⁵ In this case, Defendants failed to reasonably and adequately protect the stored records of *hundreds of millions* of patients—roughly one-third of all Americans.

74. Private Information, like that stolen from Defendants, is “often processed and packaged with other illegally obtained data to create full record sets (fullz) that contain extensive information on individuals, often in intimate detail.” The record sets are then sold on dark web sites to other criminals and “allows an identity kit to be created, which can then be sold for considerable profit to identity thieves or other criminals to support an extensive range of criminal activities.”²⁶

²³ 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>.

²⁴ Steve Adler, *Security Breaches in Healthcare in 2023*, The HIPAA Journal (January 31, 2024), https://www.hipaajournal.com/wp-content/uploads/2024/01/Security_Breaches_In_Healthcare_in_2023_by_The_HIPAA_Journal.pdf.

²⁵ See *id.*

²⁶ See *id.*

75. The American Medical Association (“AMA”) has also warned healthcare companies about the importance of protecting their patients’ confidential information:

Cybersecurity is not just a technical issue; *it’s a patient safety issue*. AMA research has revealed that 83% of physicians work in a practice that has experienced some kind of cyberattack. Unfortunately, practices are learning that *cyberattacks not only threaten the privacy and security of patients’ health and financial information, but also patient access to care*.²⁷

76. The Data Breach resulting in the theft of Plaintiffs’ and Class Members’ Private Information poses a known patient safety issue, including the interruption of important medical services.

77. Given the wealth of information from the law enforcement and healthcare industry concerning the increasing prevalence of cyberattacks, Defendants knew and should have known about its data security vulnerabilities and implemented enhanced and adequate protection to protect and secure Plaintiffs’ and Class Members’ Private Information. Knowing the risk, Defendants failed to do so.

Defendants Failure to Comply with FTC Guidelines

78. The Federal Trade Commission (“FTC”) has regularly promulgated guidelines for businesses, including HIPAA entities, which highlight the necessity of implementing reasonable data security practices. According to the FTC, the need for data security should factor into all business decision-making.

79. For example, in 2016, the FTC updated its published guidelines, *Protecting Personal Information: A Guide for Business*, which laid out standard and accepted cyber-security

²⁷ Andis Robeznieks, *Cybersecurity: Ransomware attacks shut down clinics, hospitals*, AM. MED. ASS’N (Oct. 4, 2019), <https://www.ama-assn.org/practice-management/sustainability/cybersecurity-ransomware-attacks-shut-down-clinics-hospitals>.

measures for businesses to implement to protect consumers' private data. The guidelines advise businesses, *inter alia*, to: encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.²⁸

80. The FTC's guidelines further advise businesses: not to maintain PII longer than necessary for authorization of a transaction; to limit access to sensitive data; to require complex passwords to be used on networks; to use industry-tested methods for security; to monitor for suspicious activity on the network; and to verify that third-party service providers have implemented reasonable security measures.²⁹

81. To underscore the binding significance of the promulgated guidance, the FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, pursuant to Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further identify the measures businesses *must* take to meet their data security obligations consistent with federal law.

82. These FTC enforcement actions include actions against healthcare providers and partners 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) ("[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."), *vacated on other grounds, LabMD, Inc. v. Fed. Trade Comm'n*, 894 F.3d 1221 (11th Cir. 2018).

83. Defendants' failure to employ reasonable and appropriate measures to protect against unauthorized access to patients' Private Information constitutes an unfair act or practice

²⁸ *Protecting Personal Information: A Guide for Business*, FEDERAL TRADE COMMISSION (Oct. 2016), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.

²⁹ *Id.*

prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

84. Defendants were at all times fully aware of their obligations to protect the Private Information of customers and patients. Defendants were also aware of the significant repercussions that would result from their failure to do so.

Defendants' Failure to Comply with Accepted Industry Standards for Data Security

85. In light of the evident threat of cyberattacks seeking consumers' Private Information, several best practices have been identified by regulatory agencies and experts that, at a minimum, should be implemented by healthcare service providers like Defendants to secure Plaintiffs' and Class Members' Private Information, including but not limited to: educating and training all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data; monitoring and limiting the network ports; protecting web browsers and email management systems; and limiting which employees can access sensitive data.

86. On information and belief, Defendants failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

87. These foregoing frameworks are existing and applicable industry standards in the healthcare industry, and Defendants failed to comply with these accepted standards, thereby opening the door to and causing the Data Breach.

Defendants' Failure to Comply with Their HIPAA Obligations to Safeguard Private Information

88. As healthcare service providers handling medical patient data and providing services to healthcare providers, pharmacies, and pharmaceutical companies, Defendants are covered entities under HIPAA (45 C.F.R. § 160.103) and are required to comply with the HIPAA Privacy Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and E (“Standards for Privacy of Individually Identifiable Health Information”), and Security Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and C (“Security Standards for the Protection of Electronic Protected Health Information”).

89. HIPAA requires covered entities to protect against reasonably anticipated threats to the security of sensitive patient health information.

90. Defendants are subject to the rules and regulations for safeguarding electronic forms of medical information pursuant to the Health Information Technology Act (“HITECH”). *See 42 U.S.C. § 17921, 45 C.F.R. § 160.103.*

91. HIPAA’s Privacy Rule or *Standards for Privacy of Individually Identifiable Health Information* establishes national standards for the protection of health information that is kept or transferred in electronic form.

92. HIPAA covered entities must implement safeguards to ensure the confidentiality, integrity, and availability of PHI. These safeguards include physical, technical, and administrative components.

93. The Data Breach is considered a breach under the HIPAA Rules because it involved an access of PHI not permitted under the HIPAA Privacy Rule:

A breach under the HIPAA Rules is defined as “the acquisition, access, use, or disclosure of PHI in a manner not permitted under the [HIPAA Privacy Rule] which compromises the security or privacy of the PHI.” *See 45 C.F.R. 164.40*

94. 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.

Defendants' Failure to Adequately and Reasonably Secure Plaintiffs' and Class Members' Private Information has Increased Their Risk of Fraud and Identity Theft

95. Cyberattacks and data breaches at healthcare service providers like Defendants are especially problematic because they can negatively impact the overall daily lives of individuals affected by the attack.

96. Researchers have found that, among medical service providers that experience a data security incident, the death rate among patients increased in the months and years after the attack.³⁰

97. Researchers have further found that for medical service providers that experienced a data security incident, the incident was associated with deterioration in timeliness of care and patient outcomes.³¹

98. The United States Government Accountability Office released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft face "substantial costs and time to repair the damage to their good name and credit record."³²

99. That is because any victim of a data breach is exposed to serious ramifications regardless of the nature of the data. Indeed, the reason criminals steal PII is to monetize it. They

³⁰ See Nsikan Akpan, *Ransomware and Data Breaches Linked to Uptick in Fatal Heart Attacks*, PBS (Oct. 24, 2019), <https://www.pbs.org/newshour/science/ransomware-and-other-data-breaches-linked-to-uptick-in-fatal-heart-attacks>.

³¹ See Sung J. Choi, et al., *Data Breach Remediation Efforts and Their Implications for Hospital Quality*, 54 Health Services Research 971, 971-980 (2019), available at <https://onlinelibrary.wiley.com/doi/full/10.1111/1475-6773.13203>.

³² See U.S. Gov. Accounting Office, GAO-07-737, Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown (June 2007), available at <https://www.gao.gov/new.items/d07737.pdf>.

do this by selling the spoils of their cyberattacks on the black market to identity thieves who desire to extort and harass victims, and take over victims' identities to engage in illegal financial transactions under the victims' names. Because a person's identity is akin to a puzzle, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity, or otherwise harass or track the victim. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique known as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails.

100. The FTC recommends that identity theft victims take several steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for seven years if someone steals their identity), 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.³³

101. Moreover, theft of Private Information is also gravely serious because Private Information is an extremely valuable property right.³⁴

³³ See *IdentityTheft.gov*, FEDERAL TRADE COMMISSION, <https://www.identitytheft.gov/Steps> (last visited Dec. 11, 2023).

³⁴ See, e.g., John T. Soma, et al, *Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets*, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

102. Its value is axiomatic, considering the value of “big data” in corporate America and the fact that the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that Private Information has considerable market value.

103. It must also be noted there may be a substantial time lag – measured in years – between when harm occurs and when it is discovered, and also between when Private Information and/or financial information is stolen and when it is used.

104. According to the GAO, which conducted a study regarding data breaches:

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

GAO Report at 29.

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

106. Thus, Plaintiffs and Class Members must vigilantly monitor their financial and medical accounts, or the accounts of deceased individuals for whom Class Members are the executors or surviving spouses, for many years to come.

107. Private Information can sell for as much as \$363 per record according to the Infosec Institute.³⁵ Private Information is particularly valuable because criminals can use it to target victims with frauds and scams. Once Private Information is stolen, fraudulent use of that

³⁵ See Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, InfoSec (July 27, 2015), <https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/>.

information and damage to victims may continue for years.

108. Medical information is especially valuable to identity thieves.

109. Theft of PHI, in particular, is gravely serious: “[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.”³⁶

110. Drug manufacturers, medical device manufacturers, pharmacies, hospitals, and other healthcare service providers often purchase PHI on the black market for the purpose of target marketing their products and services to the physical maladies of the data breach victims themselves. Insurance companies purchase and use wrongfully disclosed PHI to adjust their insureds’ medical insurance premiums.

111. Because of the value of its collected and stored data, the medical industry has experienced disproportionately higher numbers of data theft events than other industries.

112. For this reason, Defendants knew or should have known about these dangers and strengthened their data and email handling systems accordingly. Defendants were on notice of the substantial and foreseeable risk of harm from a data breach, yet Defendants failed to properly prepare for that risk.

Defendants’ Failure to Adequately and Reasonably Protect Against The Data Breach was Reckless and Negligent

113. Defendants breached their obligations to Plaintiffs and Class Members and/or were otherwise negligent and reckless because they failed to properly maintain and safeguard their computer systems and data to protect and/or to implement adequate data security oversight and

³⁶ See Federal Trade Commission, *What to Know About Medical Identity Theft*, <http://www.consumer.ftc.gov/articles/0171-medical-identity-theft> (last visited Dec. 11, 2023).

practices necessary to safeguard stored Private Information. Defendants' unlawful conduct includes, but is not limited to, the following acts and/or omissions:

- a. Failing to maintain an adequate data security system to reduce the risk of data breaches and cyber-attacks;
- b. Failing to adequately protect patients' and customers' Private Information;
- c. Failing to properly monitor their own data security systems for existing intrusions;
- d. Failing to ensure that their vendors with access to their computer systems and/or data employed reasonable security procedures;
- e. Failing to train their employees in the proper handling of emails containing Private Information and maintain adequate email security practices;
- f. Failing to ensure the confidentiality and integrity of electronic PHI they created, received, maintained, and/or transmitted, in violation of 45 C.F.R. § 164.306(a)(1);
- g. Failing to implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights in violation of 45 C.F.R. § 164.312(a)(1);
- h. Failing to implement policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 C.F.R. § 164.308(a)(1)(i);
- i. Failing to implement procedures to review records of information system activity regularly, such as audit logs, access reports, and security incident tracking reports in violation of 45 C.F.R. § 164.308(a)(1)(ii)(D);

- j. Failing to protect against reasonably anticipated threats or hazards to the security or integrity of electronic PHI in violation of 45 C.F.R. § 164.306(a)(2);
- k. Failing to protect against reasonably anticipated uses or disclosures of electronic PHI that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 C.F.R. § 164.306(a)(3);
- l. Failing to ensure compliance with HIPAA security standard rules by their workforces in violation of 45 C.F.R. § 164.306(a)(4);
- m. Failing to train all members of their workforces effectively on the policies and procedures regarding PHI as necessary and appropriate for the members of their workforces to carry out their functions and to maintain security of PHI, in violation of 45 C.F.R. § 164.530(b);
- n. Failing to render the electronic Private Information they maintained unusable, unreadable, or indecipherable to unauthorized individuals, as they had not encrypted the electronic PHI as specified in the HIPAA Security Rule by “the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key” (45 CFR § 164.304’s definition of “encryption”);
- o. Failing to comply with FTC guidelines for cybersecurity, in violation of Section 5 of the FTC Act;

- p. Failing to adhere to industry standards for cybersecurity as discussed above; and
- q. Otherwise breaching their duties and obligations to protect Plaintiffs' and Class Members' Private Information.

114. Defendants negligently, recklessly, and unlawfully failed to safeguard Plaintiffs' and Class Members' Private Information by allowing cyberthieves to access Defendants' computer network and systems which contained unsecured and unencrypted Private Information for multiple days.

115. Accordingly, as outlined below, Plaintiffs and Class Members now face an increased risk of fraud and identity theft. In addition, Plaintiffs and Class Members also lost the benefit of the bargain they made with Defendants.

Plaintiffs' and Class Members' Damages

116. Given the sensitivity of the Private Information involved in this Data Breach, Plaintiffs and Class Members have all suffered damages and will face a substantial risk of additional injuries for years to come, if not the rest of their lives. Defendants have done nothing to compensate Plaintiffs or Class Members for many of the injuries they have already suffered. Defendants have not demonstrated any efforts to prevent additional harm from befalling Plaintiffs and Class Members as a result of the Data Breach.

117. Plaintiffs and Class Members have been damaged by the compromise of their Private Information in the Data Breach, which is now in the hands of cybercriminals.

118. Since being notified of the Data Breach, Plaintiffs have spent time dealing with the impact of the Data Breach, valuable time Plaintiffs otherwise would have spent on other activities, including but not limited to time with their families, work and/or recreation.

119. Due to the Data Breach, Plaintiffs anticipate spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. This includes changing passwords, cancelling credit and debit cards, and monitoring her accounts for fraudulent activity.

120. Plaintiffs' and Class Members' Private Information was compromised as a direct and proximate result of the Data Breach.

121. As a direct and proximate result of Defendants' conduct, Plaintiffs and Class Members have been placed at a present, imminent, immediate, and continuing increased risk of harm from fraud and identity theft.

122. As a direct and proximate result of Defendants' conduct, Plaintiffs and Class Members have been forced to spend time dealing with the effects of the Data Breach.

123. Plaintiffs and Class Members face substantial risk of out-of-pocket fraud losses such as loans opened in their names, medical services billed in their names, tax return fraud, utility bills opened in their names, credit card fraud, and similar identity theft.

124. Plaintiffs and Class Members face substantial risk of being targeted for future phishing, data intrusion, and other illegal schemes based on Plaintiffs' and Class Members' Private Information as potential fraudsters could use that information to more effectively target such schemes to Plaintiffs and Class Members.

125. Plaintiffs and Class Members may also incur out-of-pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breach.

126. Plaintiffs and Class Members also suffered a loss of value of their Private Information when it was acquired by cyber thieves in the Data Breach. Numerous courts have

recognized the propriety of loss of value damages in similar cases.

127. Plaintiffs and Class Members were also damaged via benefit-of-the-bargain damages. Plaintiffs and Class Members overpaid for a service that was intended to be accompanied by adequate data security that complied with industry standards but was not. Part of the price Plaintiffs and Class Members paid to Defendants and/or Defendants' healthcare partners was intended to be used by Defendants to fund adequate security of their computer system(s) and Plaintiffs' and Class Members' Private Information. Thus, Plaintiffs and Class Members did not get what they paid for and agreed to.

128. Plaintiffs and Class Members have spent and will continue to spend significant amounts of time monitoring their accounts and sensitive information for misuse.

129. Plaintiffs and Class Members have suffered or will suffer actual injury as a direct result of the Data Breach. Many victims suffered ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach relating to:

- a. Reviewing and monitoring sensitive accounts and finding fraudulent insurance claims, loans, and/or government benefits claims;
- b. Purchasing credit monitoring and identity theft prevention;
- c. Placing "freezes" and "alerts" with reporting agencies;
- d. Spending time on the phone with or at financial institutions, healthcare providers, and/or government agencies to dispute unauthorized and fraudulent activity in their name;
- e. Contacting financial institutions and closing or modifying financial accounts;

and

f. Closely reviewing and monitoring Social Security Number, medical insurance accounts, bank accounts, and credit reports for unauthorized activity for years to come.

130. Moreover, Plaintiffs and Class Members have an interest in ensuring that their Private Information, which is believed to remain in the possession of Defendants, is protected from further breaches by the implementation of security measures and safeguards, including but not limited to, making sure that the storage of data or documents containing Private Information is not accessible online and that access to such data is password protected.

131. Further, as a result of Defendants' conduct, Plaintiffs and Class Members are forced to live with the anxiety that their Private Information—which contains the most intimate details about a person's life, including what ailments they suffer from, whether physical or mental—may be disclosed to the entire world, thereby subjecting them to embarrassment and depriving them of any right to privacy whatsoever.

132. Moreover, the magnitude of harm arising from this Data Breach is greater in kind and extent than harm resulting from other Data Breaches in the healthcare sector, owing to the fact that Plaintiffs and Class Members suffered injuries beyond those arising from the theft of their Private Information. Specifically, Plaintiffs and Class Members suffered harm from increased out-of-pocket expenses to obtain medical services and prescriptions, being unable to fill their prescriptions entirely, and/or not being able to apply discount coupons to afford their medications or healthcare services.

133. As a direct and proximate result of Defendants' actions and inactions, Plaintiffs and Class Members have suffered anxiety, emotional distress, loss of time, loss of privacy, and are at an increased risk of future harm.

Plaintiffs' Experiences

Plaintiff Borne's Experience

134. To use Defendants' services, Plaintiff Borne—like other Class Members—provided sensitive Private Information including her full name, address, date of birth, Social Security number, medical records, insurance information, billing, banking, and credit card information, family medical history, and more either to Defendants directly or to her healthcare providers or pharmacies to provide to Defendants.

135. Defendants obtained and continue to store and maintain Plaintiffs' and Class Members' Private Information. Defendants owe 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 Defendants' inadequate data security practices, which resulted in the Data Breach.

136. Over three months after the Data Breach, Defendants have yet to confirm the exact information that was compromised in the Data Breach. However, on information and belief, Class Members' compromised data includes, but is not limited to: patient name, address, date of birth, health diagnosis, and medications and prescriptions information.

137. Plaintiff Borne is very careful with her Private Information. She stores any documents containing her Private Information in a safe and secure location or destroys the documents. Plaintiff Borne has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source. Moreover, Plaintiff Borne diligently chooses unique usernames and passwords for her various online accounts.

138. As a result of the Data Breach, Plaintiff Borne made reasonable efforts to mitigate the impact of the Data Breach after receiving the Data Breach notification letter, including but not

limited to researching the Data Breach, reviewing credit card and financial account statements, and monitoring her credit.

139. Plaintiff Borne was forced to spend multiple hours attempting to mitigate the effects of the Data Breach. She will continue to spend valuable time she otherwise would have spent on other activities, including but not limited to time with her family, work and/or recreation. This is time that is lost forever and cannot be recaptured.

140. Plaintiff Borne suffered actual injury and damages as a result of the Data Breach including, but not limited to: (a) damage to and diminution in the value of her Private Information, a form of intangible property that Defendants obtained from Plaintiff Borne and/or Plaintiff Borne's doctors and medical professionals; (b) violation of her privacy rights; (c) the theft of her Private Information; (d) loss of time; (e) imminent and impending injury arising from the increased risk of identity theft and fraud; (f) increased out-of-pocket medical expenses; (g) failure to receive the benefit of her bargain; and (h) nominal and statutory damages.

141. Plaintiff Borne has also suffered emotional distress that is proportional to the risk of harm and loss of privacy caused by the theft of her Private Information which she believed would be protected from unauthorized access and disclosure, including anxiety about unauthorized parties viewing, selling, and/or using her Private Information for purposes of identity theft and fraud. Plaintiff Borne has also suffered anxiety about unauthorized parties viewing, using, and/or publishing information related to her health history and prescriptions. This is particularly significant given that Plaintiff Borne provided her Private Information to Defendants, in order to receive services for a condition that measurably worsens with stress.

142. As a result of the Data Breach, Plaintiff Borne anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data

Breach. In addition, Plaintiff Borne will continue to be at a present, imminent, and continued increased risk of identity theft and fraud in perpetuity.

143. Plaintiff Borne has a continuing interest in ensuring that her Private Information, which, upon information and belief, remains backed up in Defendants' possession, is protected and safeguarded from future breaches.

Plaintiff Skorupski's Experience

144. To use Defendants' services, Plaintiff Skorupski—like other Class Members—provided sensitive Private Information including her full name, address, date of birth, Social Security number, medical records, insurance information, billing, banking, and credit card information, family medical history, and more either to Defendants directly or to her healthcare providers or pharmacies to provide to Defendants.

145. Defendants obtained and continue to store and maintain Plaintiff Skorupski's and Class Members' Private Information. Defendants owe 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 Defendants' inadequate data security practices, which resulted in the Data Breach.

146. Over three months after the Data Breach, Defendants have yet to confirm the exact information that was compromised in the Data Breach. However, on information and belief, Class Members' compromised data includes, but is not limited to: patient name, address, date of birth, health diagnosis, and medications and prescriptions information.

147. Plaintiff Skorupski is very careful with her Private Information. She stores any documents containing her Private Information in a safe and secure location or destroys the documents. Plaintiff Skorupski has never knowingly transmitted unencrypted sensitive Private

Information over the internet or any other unsecured source. Moreover, Plaintiff Skorupski diligently chooses unique usernames and passwords for her various online accounts.

148. As a result of the Data Breach, Plaintiff Skorupski made reasonable efforts to mitigate the impact of the Data Breach after receiving the Data Breach notification letter, including but not limited to researching the Data Breach, reviewing credit card and financial account statements, and monitoring her credit.

149. Plaintiff Skorupski was forced to spend multiple hours attempting to mitigate the effects of the Data Breach. She will continue to spend valuable time she otherwise would have spent on other activities, including but not limited to time with her family, work and/or recreation. This is time that is lost forever and cannot be recaptured.

150. Plaintiff Skorupski suffered actual injury and damages as a result of the Data Breach including, but not limited to: (a) damage to and diminution in the value of her Private Information, a form of intangible property that Defendants obtained from Plaintiff Skorupski and/or Plaintiff Skorupski's doctors and medical professionals; (b) violation of her privacy rights; (c) the theft of her Private Information; (d) loss of time; (e) imminent and impending injury arising from the increased risk of identity theft and fraud; (f) increased out-of-pocket medical expenses;; (g) failure to receive the benefit of her bargain; and (h) nominal and statutory damages.

151. Plaintiff Skorupski has also suffered emotional distress that is proportional to the risk of harm and loss of privacy caused by the theft of her Private Information which she believed would be protected from unauthorized access and disclosure, including anxiety about unauthorized parties viewing, selling, and/or using her Private Information for purposes of identity theft and fraud. Plaintiff Skorupski has also suffered anxiety about unauthorized parties viewing, using, and/or publishing information related to her health history and prescriptions.

152. As a result of the Data Breach, Plaintiff Skorupski anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. In addition, Plaintiff Skorupski will continue to be at a present, imminent, and continued increased risk of identity theft and fraud in perpetuity.

153. Plaintiff Skorupski has a continuing interest in ensuring that her Private Information, which, upon information and belief, remains backed up in Defendants' possession, is protected and safeguarded from future breaches.

CLASS ACTION ALLEGATIONS

154. Plaintiffs bring this action against Defendants individually and on behalf of all other persons similarly situated.

155. Plaintiffs propose the following Class and Subclass definitions, subject to amendment as appropriate:

National Class: All persons or, if minors, their parents or guardians, or, if deceased, their executors or surviving spouses, who Defendants identified as being among those individuals whose Private Information was compromised in the Data Breach (the "Class").

Connecticut Subclass: All persons or, if minors, their parents or guardians, or, if deceased, their executors or surviving spouses, residing in Connecticut who Defendants identified as being among those individuals whose Private Information was compromised in the Data Breach (the "Connecticut Subclass").

Louisiana Subclass: All persons or, if minors, their parents or guardians, or, if deceased, their executors or surviving spouses, residing in Louisiana who Defendants identified as being among those individuals whose Private Information was compromised in the Data Breach (the "Louisiana Subclass").

156. Excluded from the Class (and Subclasses) are Defendants' officers, directors, and employees; any entity in which Defendants have a controlling interest; and the affiliates, legal

representatives, attorneys, successors, heirs, and assigns of Defendants. Excluded also from the Class are members of the judiciary to whom this case is assigned, their families and members of their staff.

157. Plaintiffs reserve the right to amend or modify the Class or Subclass definition or create additional subclasses as this case progresses.

158. Numerosity. The Members of the Class are so numerous that joinder of all of them is impracticable. As of May 28, 2024, over 500,000 individuals were sent.

159. Commonality. There are questions of law and fact common to the Class, which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

- a. Whether Defendants unlawfully used, maintained, lost, or disclosed Plaintiffs' and Class Members' Private Information;
- b. Whether Defendants failed to implement and maintain reasonable and adequate security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;
- c. Whether Defendants' data security systems prior to and during the Data Breach complied with applicable data security laws and regulations including, e.g., HIPAA;
- d. Whether Defendants' data security systems prior to and during the Data Breach were consistent with industry standards;
- e. Whether Defendants owed a duty to Plaintiffs and Class Members to safeguard their Private Information;

- f. Whether Defendants breached their duty to Plaintiffs and Class Members to safeguard their Private Information;
- g. Whether Defendants knew or should have known that their data security systems and monitoring processes were deficient;
- h. Whether Defendants should have discovered the Data Breach sooner;
- i. Whether Plaintiffs and Class Members suffered legally cognizable damages as a result of Defendants' misconduct;
- j. Whether Defendants' conduct was negligent;
- k. Whether Defendants breached implied contracts with Plaintiffs and Class Members;
- l. Whether Defendants were unjustly enriched by unlawfully retaining a benefit conferred upon them by Plaintiffs and Class Members;
- m. Whether Defendants failed to provide notice of the Data Breach in a timely manner, and;
- n. Whether Plaintiffs and Class Members are entitled to damages, civil penalties, punitive damages, treble damages, and/or injunctive relief.

160. Typicality. Plaintiffs' claims are typical of those of other Class Members because Plaintiffs' information, like that of every other Class Member, was compromised in the Data Breach.

161. Adequacy of Representation. Plaintiffs will fairly and adequately represent and protect the interests of the Members of the Class. Plaintiffs' Counsel are competent and experienced in litigating class actions.

162. Predominance. Defendants have engaged in a common course of conduct toward Plaintiffs and Class Members, in that all the data of Plaintiffs and Class Members was stored on the same network and unlawfully accessed in the same way. The common issues arising from Defendants' conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

163. Superiority. A class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Defendants. In contrast, to conduct this action as a class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class Member.

164. 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 classwide basis.

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

- a. Whether Defendants failed to timely notify the public of the Data Breach;

- b. Whether Defendants owed a legal duty to Plaintiffs and the Class to exercise due care in collecting, storing, and safeguarding their Private Information;
- c. Whether Defendants' security measures to protect their data systems were reasonable and adequate in light of best practices recommended by data security experts;
- d. Whether Defendants' failure to institute adequate protective security measures amounted to negligence;
- e. Whether Defendants failed to take commercially reasonable steps to safeguard consumer Private Information; and
- f. Whether adherence to FTC data security recommendations, and measures recommended by data security experts would have reasonably prevented the Data Breach.

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

CLAIMS FOR RELIEF

COUNT I **Negligence and Negligence Per Se** ***(On Behalf of Plaintiffs and the Class)***

167. Plaintiffs re-allege and incorporate by reference factual allegations above as if fully set forth herein.

168. By collecting and storing the Private Information of Plaintiffs and Class Members, in their computer systems and networks, and sharing it and using it for commercial gain,

Defendants owed a duty of care to use reasonable means to secure and safeguard their computer systems—and Class Members’ Private Information held within it—to prevent disclosure of the information, and to safeguard the information from theft. Defendants’ duty included a responsibility to implement processes by which they could detect a breach of their security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a data breach.

169. 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, and the personnel responsible for them, adequately protected the Private Information.

170. Plaintiffs and Class Members are a well-defined, foreseeable, and probable group of patients that Defendants were aware, or should have been aware, could be injured by inadequate data security measures.

171. Defendants’ duty of care to use reasonable and adequate security measures arose as a result of the special relationship that existed between Defendants and consumers, which is recognized by laws and regulations including but not limited to HIPAA, the FTC Act, and common law. Defendants were in a superior position to ensure that their systems were sufficient to protect against the foreseeable risk of harm to Plaintiffs and Class Members from a data breach.

172. 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)(1). Some or all of the medical information at issue in this case constitutes “protected health information” within the

meaning of HIPAA.

173. In addition, 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.

174. Defendants’ duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendants are bound by industry standards to protect confidential Private Information.

175. Defendants breached their duties, and thus were negligent, by failing to use reasonable measures to protect Plaintiffs’ and Class Members’ Private Information. The specific negligent acts and omissions committed by Defendants include, but are not limited to, the following:

- a. Failing to adopt, implement, and maintain reasonable and adequate security measures to safeguard Plaintiffs’ and Class Members’ Private Information;
- b. Failing to adequately monitor the security of their networks and systems;
- c. Failing to ensure that their email systems had reasonable data security safeguards in place;
- d. Failing to have in place reasonable and adequate mitigation policies and procedures;
- e. Allowing unauthorized access to Plaintiffs’ and Class Members’ Private Information;
- f. Failing to detect in a timely manner that Plaintiffs’ and Class Members’ Private Information had been compromised; and

g. Failing to timely notify Plaintiffs and Class Members about the Data Breach so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

176. Plaintiffs and Class Members have no ability to protect their Private Information that was or remains in Defendants' possession.

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

178. It was therefore foreseeable that the failure to adequately safeguard Plaintiffs' and Class Members' Private Information would result in one or more types of injuries to Plaintiffs and Class Members.

179. Defendants' conduct was grossly negligent and departed from reasonable standards of care, including but not limited to, failing to adequately protect the Private Information, and failing to provide Plaintiffs and Class Members with timely notice that their sensitive Private Information had been compromised.

180. Neither Plaintiffs nor Class Members contributed to the Data Breach and subsequent misuse of their Private Information as described in this Complaint.

181. Plaintiffs and Class Members are also entitled to injunctive relief requiring Defendants to, *inter alia*, (i) strengthen their data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) continue to provide adequate credit monitoring to all Class Members.

182. The injury and harm Plaintiffs and Class Members suffered was the reasonably foreseeable result of Defendants' breach of their duties. Defendants knew or should have known that they were failing to meet their duties, and that Defendants' breach would cause Plaintiffs and Class Members to experience the foreseeable harms associated with the exposure of their Private Information.

183. As a direct and proximate result of Defendants' negligent conduct, Plaintiffs and Class Members have suffered injury and are entitled to compensatory and consequential damages in an amount to be proven at trial.

COUNT II
Breach of Implied Contract
(On behalf of Plaintiffs and the Class)

184. Plaintiffs re-allege and incorporate by reference factual allegations above as if fully set forth herein.

185. Defendants acquired and maintained the Private Information of Plaintiffs and the Class that they received either directly or from their healthcare providers.

186. When Plaintiffs and Class Members paid money and provided their Private Information to their doctors and/or healthcare providers, including their pharmacies, pharmaceutical companies, or patient support programs like BMS, either directly or indirectly, in exchange for goods or services, they entered into implied contracts with their doctors and/or healthcare professionals, their business associates, and partners, including Defendants.

187. Plaintiffs and Class Members entered into implied contracts with Defendants under which Defendants agreed to safeguard and protect such information and to timely and accurately notify Plaintiffs and Class Members that their information had been breached and compromised.

188. Plaintiffs and the Class were required to deliver their Private Information to Defendants as part of the process of obtaining services provided by Defendants, either directly or indirectly. Plaintiffs and Class Members paid money, or money was paid on their behalf, to Defendants in exchange for services.

189. Defendants directly or indirectly solicited, offered, and invited Class Members to provide their Private Information as part of Defendants' regular business practices. Plaintiffs and Class Members accepted Defendants offers and provided their Private Information to Defendants or, alternatively, provided their information to doctors or other healthcare professionals, who then provided it to Defendants.

190. Defendants accepted possession of Plaintiffs' and Class Members' Private Information for the purpose of providing services to Plaintiffs and Class Members and/or their doctors and other healthcare professionals.

191. In accepting such information and payment for services, Defendants entered into implied contracts with Plaintiffs and Class Members whereby Defendants became obligated to reasonably safeguard Plaintiffs' and Class Members' Private Information.

192. Alternatively, Plaintiffs and Class Members were the intended beneficiaries of data protection agreements entered into between Defendants and healthcare providers, including pharmacies, pharmaceutical companies, and patient support programs.

193. In delivering, directly or indirectly, their Private Information to Defendants and paying for healthcare services, Plaintiffs and Class Members intended and understood that Defendants would adequately safeguard the data as part of that service.

194. The implied promise of confidentiality includes consideration beyond those pre-existing general duties owed under HIPAA or other state or federal regulations. The additional

consideration included implied promises to take adequate steps to comply with specific industry data security standards and FTC guidelines on data security.

195. The implied promises include but are not limited to: (1) taking steps to ensure that any agents who are granted access to Private Information also protect the confidentiality of that data; (2) taking steps to ensure that the information that is placed in the control of their agents is restricted and limited to achieve an authorized medical purpose; (3) restricting access to qualified and trained agents; (4) designing and implementing appropriate retention policies to protect the information against criminal data breaches; (5) applying or requiring proper encryption; (6) multifactor authentication for access; and (7) other steps to protect against foreseeable data breaches.

196. Plaintiffs and Class Members (or their healthcare providers) would not have entrusted their Private Information to Defendants in the absence of such an implied contract.

197. Had Defendants disclosed to Plaintiffs and Class Members (or their doctors and healthcare providers) that they did not have adequate computer systems and security practices to secure sensitive data, Plaintiffs and Class Members (or their doctors and healthcare providers) would not have provided their Private Information to Defendants.

198. Defendants recognized that Plaintiffs' and Class Members' Private Information is highly sensitive and must be protected, and that this protection was of material importance as part of the bargain with Plaintiffs and Class Members (or their doctors and healthcare providers).

199. Plaintiffs and Class Members (or their doctors and healthcare providers) fully performed their obligations under the implied contracts with Defendants.

200. Defendants breached the implied contracts with Plaintiffs and Class Members (or their doctors and healthcare providers) by failing to take reasonable and adequate measures to

safeguard their Private Information as described herein.

201. As a direct and proximate result of Defendants' conduct, Plaintiffs and Class Members suffered and will continue to suffer damages in an amount to be proven at trial.

COUNT III

Breach of Contractual Duties Owed to Third-Party Beneficiaries
(On Behalf of Plaintiffs and the Class against Defendants Cencora and Lash Group)

202. Plaintiffs incorporate and realleges all factual allegations above as if fully set forth herein.

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

204. These contracts were made expressly for the benefit of Plaintiffs and the Class, as it was their confidential medical information that Defendants agreed to collect and protect through its services. Thus, the benefit of collection and protection of the Private Information belonging to Plaintiffs and the Class was the direct and primary objective of the contracting parties.

205. Defendants 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.

206. Defendants 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.

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

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

COUNT IV
Unjust Enrichment
(On Behalf of Plaintiffs and the Class)

209. Plaintiffs re-allege and incorporate by reference all factual allegations above as if fully set forth herein.

210. This count is pleaded in the alternative to the breach of contract claims (Counts II and III).

211. Upon information and belief, Defendants fund any data security measures they implement entirely from their general revenue, including from money they make based upon representations of protecting Plaintiffs' and Class Members' Private Information.

212. There is a direct nexus between money paid to Defendants and the requirement that Defendants keep Plaintiffs' and Class Members' Private Information confidential and protected.

213. Plaintiffs and Class Members paid Defendants and/or healthcare providers a certain sum of money, which was used to fund any data security measures implemented by Defendants via contracts with Defendants.

214. As such, a portion of the payments made by or on behalf of Plaintiffs and Class Members is to be used to provide a reasonable and adequate level of data security, and the amount

of the portion of each payment made that is allocated to data security is known to Defendants.

215. Protecting the Private Information of Plaintiffs and Class Members is integral to Defendants' businesses. Without their data, Defendants would be unable to provide the healthcare-related services to pharmacies, pharmaceutical companies, healthcare providers, or patient support programs comprising Defendants' core business.

216. Plaintiffs' and Class Members' data and Private Information has monetary value.

217. Plaintiffs and Class Members directly and indirectly conferred a monetary benefit on Defendants. They indirectly conferred a monetary benefit on Defendants by purchasing goods and/or services from entities that contracted with Defendants, and from which Defendants received compensation to protect certain data. Plaintiffs and Class Members directly conferred a monetary benefit on Defendants by supplying Private Information, which has value, from which value Defendants derive their business value, and which should have been protected with adequate data security.

218. Defendants knew that Plaintiffs and Class Members conferred a benefit which Defendants accepted. Defendants profited from these transactions and used the Private Information of Plaintiffs and Class Members for business purposes.

219. Defendants enriched themselves by saving the costs they reasonably should have expended on adequate data security measures to secure Plaintiffs' and Class Members' Private Information. Instead of providing a reasonable and adequate level of security that would have prevented the Data Breach, Defendants instead chose to shirk their data security obligations to increase profits at the expense of Plaintiffs and Class Members by utilizing cheaper, ineffective data security measures. Plaintiffs and Class Members suffered as a direct and proximate result of Defendants' calculated failures to provide the requisite reasonable and adequate data security.

220. Under the principles of equity and good conscience, Defendants should not be permitted to retain the money belonging to Plaintiffs and Class Members, because Defendants failed to implement reasonable and adequate data management and security measures that are mandated by federal law and industry standards.

221. Defendants acquired the monetary benefit and Private Information through inequitable means in that they failed to disclose the inadequate security practices previously alleged.

222. If Plaintiffs and Class Members knew that Defendants had not secured their Private Information, they would not have agreed to provide their Private Information to Defendants (or to their physician to provide to Defendants).

223. Plaintiffs and Class Members have no adequate remedy at law.

224. As a direct and proximate result of Defendants' conduct, Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity to control how their Private Information is used; (iii) the compromise, publication, and/or theft of their Private Information; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their Private Information; (v) lost opportunity costs associated with effort expended and loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (vi) the continued risk to their Private Information, which remain in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect Private Information in their continued possession; (vii) loss or privacy from the authorized access and exfiltration of

their Private Information; and (viii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the Private Information compromised as a result of the Data Breach for the remainder of the lives of Plaintiffs and Class Members.

225. As a direct and proximate result of Defendants' conduct, Plaintiffs and Class Members have suffered and will continue to suffer other forms of injury and/or harm.

226. Defendants should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiffs and Class Members, proceeds that they unjustly received from them. In the alternative, Defendants should be compelled to refund the amounts that Plaintiffs and Class Members overpaid for Defendants' services.

COUNT V
Bailment
(On Behalf of Plaintiffs and the Class)

227. Plaintiffs re-allege and incorporate by reference all factual allegations above as if fully set forth herein.

228. Plaintiffs and Class Members provided Private Information to Defendants—either directly or through healthcare providers and their business associates—which Defendants were under a duty to keep private and confidential.

229. Plaintiffs' and Class Members' Private Information is personal property, and was conveyed to Defendants for the certain purpose of keeping the information private and confidential.

230. Plaintiffs' and Class Members' Private Information has value and is highly prized by hackers and criminals. Defendants were aware of the risks they took when accepting the Private Information for safeguarding and assumed the risk voluntarily.

231. Once Defendants accepted Plaintiffs' and Class Members' Private Information, they were in the exclusive possession of that information, and neither Plaintiffs nor Class Members could control that information once it was within the possession, custody, and control of Defendants.

232. Defendants did not safeguard Plaintiffs' or Class Members' Private Information when they failed to adopt and implement reasonable and adequate data security safeguards to prevent the known risk of a cyberattack.

233. Defendants' failure to safeguard Plaintiffs' and Class Members' Private Information resulted in that information being accessed or obtained by third-party cybercriminals.

234. As a result of Defendants' failure to keep Plaintiffs' and Class Members' Private Information secure, Plaintiffs and Class Members suffered injury, for which compensation—including nominal damages and compensatory damages—are appropriate.

COUNT VI
Breach of Fiduciary Duty
(On Behalf of Plaintiffs and the Class)

235. Plaintiffs re-allege and incorporate by reference all factual allegations above as if fully set forth herein.

236. In light of the special relationship between Defendants and Plaintiffs and Class Members, Defendants became fiduciaries by undertaking a guardianship of the Private Information to act primarily for Plaintiffs and Class Members: (1) for the safeguarding of Plaintiffs' and Class Members' Private Information; (2) to timely notify Plaintiffs and Class Members of a Data Breach and disclosure; and (3) to maintain complete and accurate records of what information (and where) Defendants do store.

237. Defendants had a fiduciary duty to act for the benefit of Plaintiffs and Class Members upon matters within the scope of their relationship with patients (or the patients of their healthcare clients), in particular, to keep secure their Private Information.

238. Defendants breached their fiduciary duty to Plaintiffs and Class Members by failing to encrypt and otherwise protect the integrity of the systems containing Plaintiffs' and Class Members' Private Information.

239. Defendants breached their fiduciary duty to Plaintiffs and Class Members by otherwise failing to safeguard Plaintiffs' and Class Members' Private Information.

240. As a direct and proximate result of Defendants' breach of their fiduciary duties, Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the compromise, publication, and/or theft of their Private Information; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their Private Information; (iv) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (v) the continued risk to their Private Information, which 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 in their continued possession; (vi) future costs in terms of time, effort, and money that will be expended as result of the Data Breach for the remainder of the lives of Plaintiffs and Class Members; and (vii) the diminished value of Defendants' services they received.

241. As a direct and proximate result of Defendants' breach of their fiduciary duties, Plaintiffs and Class Members have suffered and will continue to suffer other forms of injury and/or

harm, and other economic and non-economic losses.

COUNT VII
Connecticut Unfair Trade Practices Act
C.G.S.A. § 42-110G
(On Behalf of Plaintiff Skorupski and the Connecticut Subclass)

242. Plaintiff Skorupski (“Plaintiff,” for purposes of this Count), individually and on behalf of the Connecticut Subclass, repeats and alleges factual allegations, as if fully alleged herein.

243. Defendants are each a “person” as defined by C.G.S.A. § 42-110a(3).

244. Defendants are engaged in “trade” or “commerce” as those terms are defined by C.G.S.A. § 42-110a(4).

245. Upon filing this Complaint, Plaintiff will promptly send notice to the Attorney General and Commissioner of Consumer Protection pursuant to C.G.S.A. § 42-110g(c). Plaintiff will provide a file-stamped copy of the Complaint to the Attorney General and Commissioner of Consumer Protection.

246. Defendants advertised, offered, or sold services in Connecticut, and engaged in trade or commerce directly or indirectly affecting the people of Connecticut. Defendants engaged in deceptive acts and practices and unfair acts and practices in the conduct of trade or commerce, in violation of the C.G.S.A. § 42-110b, including:

- a. Representing that services have sponsorship, approval, characteristics, ingredients, uses, benefits, or qualities that they do not have;
- b. Representing that services are of a particular standard, quality, or grade, or that goods are of a particular style or model, if they are of another; and
- c. Engaging in any other unconscionable, false, misleading, or deceptive act or practice in the conduct of trade or commerce.

247. Defendants' representations and omissions were material because they were likely to deceive reasonable consumers.

248. Defendants intended to mislead Plaintiff and Connecticut Subclass members and induce them to rely on its misrepresentations and omissions.

249. Had Defendants disclosed to Plaintiff and Connecticut Subclass members that they misrepresented the security utilized on its networks, or otherwise had not omitted to Plaintiff and Connecticut Subclass members that its systems were insecure, Defendants would not have been able to continue storing Plaintiff and Connecticut Subclass members' Private Information on their networks and would have been forced to disclose the material information regarding security. Instead, Defendants allowed their servers to be hacked—undetected—and failed to discover that its servers were vulnerable through adequate due diligence and testing, and yet still continued to store customers' Private Information in its databases.

250. Defendants' unlawful, deceptive, and unconscionable acts include:

- a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and class members' Private Information, which was a direct and proximate cause of the Data Breach;
- b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;
- c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Connecticut Subclass members' Private Information;

- d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Connecticut Subclass members' Private Information, including by implementing and maintaining reasonable security measures;
- e. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Connecticut class members' Private Information;
- f. Omitting, suppressing, and concealing the material fact that they did not reasonably or adequately secure Plaintiff and Connecticut Subclass members' Private Information; and
- g. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Connecticut Subclass members' Private Information.

251. Defendants' conduct is intentional, knowing, and malicious because Defendants knew the value of Private Information they stored and failed to undertake or implement necessary safeguards, controls, and data security measures to keep it secure.

252. As a direct and proximate result of Defendants' deceptive acts and practices, Plaintiff and Connecticut Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from identity theft, fraudulent charges, and time and money spent on preventative and corrective measures.

253. Defendants' deceptive acts and practices caused substantial, ascertainable injury to Plaintiff and Connecticut Subclass members, which they could not reasonably avoid, and which outweighed any benefits to consumers or to competition.

254. Defendants' violations of Connecticut law were done with reckless indifference to Plaintiff and the Connecticut Subclass or was with an intentional or wanton violation of those rights.

255. Plaintiff requests damages in the amount to be determined at trial, including statutory and common law damages, restitution, attorneys' fees, and punitive damage.

COUNT VIII
Louisiana Unfair Trade Practices and Consumer Protection Law
La. Rev. Stat. Ann. §§ 51:1401, *et seq.*
(On Behalf of Plaintiff Borne and the Louisiana Subclass)

256. Plaintiff Borne ("Plaintiff," for purposes of this Count), individually and on behalf of the Louisiana Subclass, repeats and alleges all factual allegations as if fully alleged herein.

257. Defendants, Plaintiff, and the Louisiana Subclass members are "persons" within the meaning of the La. Rev. Stat. Ann. § 51:1402(8).

258. Plaintiff and Louisiana Subclass members are "consumers" within the meaning of La. Rev. Stat. Ann. § 51:1402(1).

259. Defendants engaged in "trade" or "commerce" within the meaning of La. Rev. Stat. Ann. § 51:1402(10).

260. The Louisiana Unfair Trade Practices and Consumer Protection Law ("Louisiana CPL") makes unlawful "unfair or deceptive acts or practices in the conduct of any trade or commerce." La. Rev. Stat. Ann. § 51:1405(A). Unfair acts are those that offend established public policy, while deceptive acts are practices that amount to fraud, deceit, or misrepresentation.

261. Defendants participated in unfair and deceptive acts and practices that violated the Louisiana CPL, including:

- a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Louisiana Subclass members' Private Information,

which was a direct and proximate cause of the Data Breach;

- b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;
- c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Louisiana Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;
- d. Misrepresenting that they would protect the privacy and confidentiality of Plaintiff and Louisiana Subclass members' Private Information, including by implementing and maintaining reasonable security measures;
- e. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Louisiana Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45 and HIPAA;
- f. Omitting, suppressing, and concealing the material fact that they did not reasonably or adequately secure Plaintiff and Louisiana Subclass members' Private Information; and
- g. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Louisiana Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45 and HIPAA.

262. Defendants' representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendants' data security and ability to protect the confidentiality of consumers' Private Information.

263. Defendants intended to mislead Plaintiff and Louisiana Subclass members and induce them to rely on its misrepresentations and omissions.

264. Defendants' unfair and deceptive acts and practices were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to Plaintiff and Louisiana Subclass members that they could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

265. Defendants acted intentionally, knowingly, and maliciously to violate Unfair Trade Practices and Consumer Protection Law, and recklessly disregarded Plaintiff and Louisiana Subclass members' rights.

266. Had Defendants disclosed to Plaintiffs and Louisiana Subclass members that its data systems were not secure and, thus, vulnerable to attack, Defendants would have been unable to continue in business and they would have been forced to adopt reasonable data security measures and comply with the law. Instead, Defendants received, maintained, and compiled Plaintiff's and Louisiana Subclass members' Private Information as part of the services Defendants provided and for which Plaintiff and Louisiana Subclass members paid without advising Plaintiff and Louisiana Subclass members that Defendants' data security practices were insufficient to maintain the safety and confidentiality of Plaintiffs' and class members' Private Information. Accordingly, Plaintiff and the Louisiana Subclass members acted reasonably in relying on Defendants misrepresentations and omissions, the truth of which they could not have discovered.

267. As a direct and proximate result of Defendants' unfair and deceptive acts and practices, Plaintiff and Louisiana Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including loss of the benefit of their bargain with Defendants as they would not have paid Defendants for goods and services or would have paid less for such goods and services but for Defendants' violations alleged herein; losses from fraud and identity theft; costs for credit monitoring and identity protection services; time and expenses related to monitoring their financial accounts for fraudulent activity; time and money spent cancelling and replacing passports; loss of value of their Private Information; and an increased, imminent risk of fraud and identity theft.

268. Plaintiff and Louisiana Subclass members seek all monetary and non-monetary relief allowed by law, including actual damages; treble damages for Defendants' knowing violations of the Louisiana CPL; restitution; declaratory relief; attorneys' fees; and any other relief that is just and proper.

COUNT IX
Louisiana Database Security Breach Notification Law
La. Rev. State. Ann. §§ 51:3074(A), et seq
(*On Behalf of Plaintiff Borne and the Louisiana Subclass*)

269. Plaintiff Borne ("Plaintiff," for purposes of this Count), individually and on behalf of the Louisiana Subclass, repeats and alleges all factual allegations as if fully alleged herein.

270. Defendants are businesses that own or license computerized data that includes Private Information as defined by La. Rev. Stat. Ann. § 51:3074(C).

271. Plaintiff's and Louisiana Subclass members' Private Information includes Private Information as covered under La. Rev. Stat. Ann. § 51:3074(C).

272. Defendants are required to accurately notify Plaintiff and Louisiana Subclass members if they become aware of a breach of their data security system that was reasonably likely

to have caused unauthorized persons to acquire Plaintiff's and Louisiana Subclass members' Private Information, in the most expedient time possible and without unreasonable delay under La. Rev. Stat. Ann. § 51:3074(C).

273. Because Defendants were aware of a breach of their security system that was reasonably likely to have caused unauthorized persons to acquire Plaintiff's and Louisiana Subclass members' Private Information, Defendants had an obligation to disclose the Data Breach in a timely and accurate fashion as mandated by La. Rev. Stat. Ann. § 51:3074(C).

274. By failing to disclose the Data Breach in a timely and accurate manner, Defendants violated La. Rev. Stat. Ann. § 51:3074(C).

275. As a direct and proximate result of Defendants' violations of La. Rev. Stat. Ann. § 51:3074(C), Plaintiff and Louisiana Subclass members suffered damages, as described above.

276. Plaintiff and Louisiana Subclass members seek relief under La. Rev. Stat. Ann. § 51:3075, including actual damages.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs pray for judgment as follows:

- a) For an Order certifying this action as a Class Action and appointing Plaintiffs as Class Representatives and their counsel as Class Counsel;
- b) For equitable relief enjoining Defendants from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiffs' and Class Members' Private Information, and from refusing to issue prompt, complete and accurate disclosures to Plaintiffs and Class Members;
- c) For equitable relief compelling Defendants to utilize appropriate methods and policies with respect to consumer data collection, storage, and safety, and to disclose with

specificity the type of Private Information compromised during the Data Breach;

- d) For equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendants' wrongful conduct;
- e) Ordering Defendants to pay for not less than five years of credit monitoring services for Plaintiffs and the Class;
- f) For an award of actual damages, compensatory damages, statutory damages, nominal damages, and/or statutory penalties, in an amount to be determined, as allowable by law;
- g) For an award of punitive damages, as allowable by law;
- h) Pre- and post-judgment interest on any amounts awarded; and,
- i) Such other and further relief as this court may deem just and proper.

JURY TRIAL DEMANDED

Under Federal Rule of Civil Procedure 38(b), Plaintiffs demand a trial by jury of any and all issues in this action so triable as of right.

Dated: June 4, 2024

Respectfully submitted,

/s/ Jeannine M. Kenney
Jeannine M. Kenney (PA Bar Id.
307635)
HAUSFELD LLP
325 Chestnut Street, Suite 900
Philadelphia, PA 19106
T: (215) 985-3270
F: (215) 985-3271
jkenney@hausfeld.com

/s/ Mindee J. Reuben
Mindee J. Reuben (PA Bar Id. 75308)
**LITE DEPALMA GREENBERG &
AFANADOR, LLC**
1515 Market Street, Suite 1200
Philadelphia, PA 19102

Tel: 215-854-4060
Fax: 973-623-0858
mreuben@litedepalma.com

Joseph J. DePalma*
LITE DEPALMA GREENBERG & AFANADOR, LLC
570 Broad Street, Suite 1201
Newark, NJ 07102
Tel: 973-623-3000
Fax: 973-623-0858
jdepalma@litedepalma.com

James J. Pizzirusso*
Mandy Boltax*
HAUSFELD LLP
888 16th Street, N.W., Suite 300
Washington, D.C. 20006
(202) 540-7200
jpizzirusso@hausfeld.com
mboltax@hausfeld.com

Steven M. Nathan*
Ashley Crooks*
HAUSFELD LLP
33 Whitehall Street, Fourteenth Floor
New York, NY 10004
(646) 357-1100
snathan@hausfeld.com
acrooks@hausfeld.com

Counsel for Plaintiffs

**Pro Hac Vice Forthcoming*

EXHIBIT A



Return Mail Processing
PO Box 589
Claysburg, PA 16625-0589

May 17, 2024

L3295-L01-2222017 T07063 P125 *****5-DIGIT 70785
MARILYN BORNE [REDACTED]



Re: Notice of Data Security Incident

Dear Marilyn Borne:

Cencora, Inc. and its Lash Group affiliate, partner with pharmaceutical companies, pharmacies, and healthcare providers to facilitate access to therapies through drug distribution, patient support services, business analytics and technology, and other services. We take very seriously the protection of the information entrusted to us in providing these services.

We are writing to let you know about an event that involved your personal information that Lash Group has through the patient support and access programs it manages on behalf of Bristol Myers Squibb and/or the Bristol Myers Squibb Patient Assistance Foundation. It is important to note that we have no evidence at this time that your information has been disclosed for any purpose other than intended to support administration of the program(s) to which you are/were enrolled, however, as a result of this incident, we are taking precautionary measures and sending this letter to tell you what happened, what information was potentially involved, what we have done and what you can do to address this situation. Please read this letter carefully, because it provides details about what happened and what we are doing about it.

What Happened?

On February 21, 2024, Cencora learned that data from its information systems had been exfiltrated, some of which could contain personal information. Upon initial detection of the unauthorized activity, Cencora immediately took containment steps and commenced an investigation with the assistance of law enforcement, cybersecurity experts and outside lawyers. On April 10, 2024, we confirmed that some of your personal information was affected by the incident.

What Information Was Involved?

Based on our investigation, personal information was affected, including potentially your first name, last name, address, date of birth, health diagnosis, and/or medications and prescriptions. There is no evidence that any of this information has been or will be publicly disclosed, or that any information was or will be misused for fraudulent purposes as a result of this incident, but we are communicating this to you so that you can take the steps outlined below to protect yourself.

What We Are Doing

Immediately upon learning of this incident, we launched an investigation with the assistance of cybersecurity experts, law enforcement, and outside lawyers. Determining whether personal information or personal health information was compromised in any way has been one of the top priorities of this effort so that we could notify potentially affected individuals. Please be assured that we are also working with cybersecurity experts to reinforce our systems and information security protocols in an effort to avoid incidents like this from occurring in the future.

2222017



We are also making resources available to those individuals whose information was involved. While we have no reason to believe that your information was used for any fraudulent purpose as a result of this incident, to help protect your identity, we are providing you with access to Experian IdentityWorksSM credit monitoring and remediation services for 24 months at no charge to you. These services provide you with alerts for two years from the date of enrollment when changes occur to your credit file. These services also provide you with proactive fraud assistance to help with any questions that you might have and identity restoration assistance in the event that you become a victim of fraud.

How do I enroll for the free services?

While identity restoration assistance is immediately available to you, we also encourage you to activate the fraud detection and credit monitoring tools available through Experian IdentityWorks. To enroll in these services at no charge, visit www.experianidworks.com/plus and follow the instructions provided. When prompted please provide the following unique code to receive services: KRTZ97HPQT. In order for you to receive the monitoring services described above, you must enroll by August 30, 2024. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.

Should you have any questions regarding the Credit Monitoring services, have difficulty enrolling, or require additional support, please contact Experian at 1-833-918-1728. Be prepared to provide engagement number B122898 as proof of eligibility for the Identity Restoration services by Experian.

What You Can Do

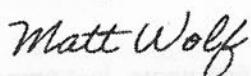
To help protect your personal information, we strongly recommend you take the following steps, all of which are good ideas in any event:

- Enroll in the credit monitoring service that we are offering to you. This will enable you to get alerts about any efforts to use your name and social security number to establish credit and restoration assistance if you were not the one who initiated it.
- Carefully review statements sent to you by your bank, credit card company, or other financial institutions as well as government institutions like the Internal Revenue Service (IRS). Notify the sender of these statements immediately by phone and in writing if you detect any suspicious transactions or other activity you do not recognize.
- The attached **Reference Guide** describes additional steps that you can take and provides resources for additional information. We encourage you to read and follow these steps as well.

For More Information

If you have questions or concerns or learn of any suspicious activity that you believe may be related to this incident, please call 1-833-918-1728. Please know that we take this matter very seriously, and we apologize for the concern and inconvenience this may cause you.

Sincerely,



Matthew Wolf
President, Biopharma Services
Lash Group

REFERENCE GUIDE

If you suspect that you are a victim of identity theft or credit fraud, we encourage you to remain vigilant and consider taking the following steps:

Order Your Free Credit Report. To order your free credit report, visit www.annualcreditreport.com, call toll-free at 877-322-8228, or complete the Annual Credit Report Request Form on the FTC's website at www.ftc.gov and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. Do not contact the three credit bureaus individually; they provide your free report only through the website or toll-free number. When you receive your credit report, review the entire report carefully. Look for any inaccuracies and/or accounts you don't recognize and notify the credit bureaus as soon as possible if there are any.

You have rights under the federal Fair Credit Reporting Act ("FCRA"). These include, among others, the right to know what is in your file; to dispute incomplete or inaccurate information; and to have consumer credit reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information about the FCRA, please visit <https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf> or www.ftc.gov

Place a Fraud Alert on Your Credit File: A fraud alert helps protect you against the possibility of an identity thief opening new credit accounts in your name. When a merchant checks the credit history of someone applying for credit, the merchant gets a notice that the applicant may be a victim of identity theft. The alert notifies the merchant to take steps to verify the identity of the applicant. You can report potential identity theft to all three of the major credit bureaus by calling any one of the toll-free fraud numbers below.

Equifax	Experian	TransUnion
www.equifax.com	www.experian.com	www.transunion.com
1-800-525-6285	1-888-397-3742	1-800-680-7289
P.O. Box 740241 Atlanta, Georgia 30374-0241	P.O. Box 9532 Allen, Texas 75013	Fraud Victim Assistance Division P.O. Box 2000 Chester, Pennsylvania 19016

Place a Security Freeze on Your Credit File. You have the right to place a "security freeze" on your credit file. A security freeze generally will prevent creditors from accessing your credit file at the three nationwide credit bureaus without your consent. You can request a security freeze free of charge by contacting the credit bureaus using the same contact information noted above.

The credit bureaus may require that you provide proper identification prior to honoring your request. In order to request a security freeze, you will need to provide: (1) Your full name (including middle initial as well as Jr., Sr., II, III, etc.); (2) Social Security number; (3) Date of birth; (4) If you have moved in the past five (5) years, provide the addresses where you have lived over the prior five years; (5) Proof of current address, such as a current utility bill or telephone bill; (6) A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.); and (7) If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to law enforcement agency concerning identity theft.

Placing a security freeze on your credit file may delay, interfere with, or prevent timely approval of any requests you make for credit, loans, employment, housing or other services. For more information regarding credit freezes, please contact the credit reporting agencies directly.

Contact the U.S. Federal Trade Commission. If you detect any incident of identity theft or fraud, promptly report the incident to your local law enforcement authorities, your state Attorney General and the Federal Trade Commission ("FTC"). If you believe your identity has been stolen, the FTC recommends that you take these additional steps.

- Close the accounts that you have confirmed or believe have been tampered with or opened fraudulently. Use the FTC's ID Theft Affidavit (available at www.ftc.gov/idtheft) when you dispute new unauthorized accounts.
- File a local police report. Obtain a copy of the police report and submit it to your creditors and any others that may require proof of the identity theft crime.



EXHIBIT B

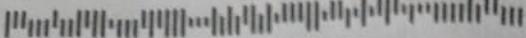
cencora

Return Mail Processing
PO Box 589
Claysburg, PA 16625-0589

May 21, 2024

546111
55821

.....AUTO**5-DIGIT 06011



CELIA SKORUPSKI



Michelle 5/28
went que into
tome on how
got

Re: Notice of Data Security Incident

Dear Celia Skorupski:

Cencora, Inc. and its Lash Group affiliate partner 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. We take very seriously the protection of the information entrusted to us in providing these services.

We are writing to let you know about an event that involved your personal information that Lash Group has obtained through its partnership with one such organization in connection with its patient support programs. It is important to note that we have no evidence at this time that your information has been used for any fraudulent purpose as a result of this incident, but we are sending this letter to tell you what happened, what information was potentially involved, what we have done and what you can do to address this situation. Please read this letter carefully, because it provides details about what happened and what we are doing about it.

What Happened?

On February 21, 2024, Cencora learned that data from its information systems had been exfiltrated, some of which could contain personal information. Upon initial detection of the unauthorized activity, Cencora immediately took containment steps and commenced an investigation with the assistance of law enforcement, cybersecurity experts and outside lawyers. On April 10, 2024, we confirmed that some of your personal information was affected by the incident.

What Information Was Involved?

Based on our investigation, your personal information was affected, including potentially your first name, last name, address, date of birth, health diagnosis, and/or medications and prescriptions. There is no evidence that any of this information has been or will be publicly disclosed, or that any information was or will be misused for fraudulent purposes as a result of this incident, but we are communicating this to you so that you can take the steps outlined below to protect yourself.

B123340



L3565-L01

INSTRUCTIONS FOR ATTORNEYS COMPLETING CIVIL COVER SHEET FORM JS 44**Authority For Civil Cover Sheet**

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

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

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

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

II. Jurisdiction. The basis of jurisdiction is set forth under Rule 8(a), F.R.Cv.P., which requires that jurisdictions be shown in pleadings. Place an "X" in one of the boxes. If there is more than one basis of jurisdiction, precedence is given in the order shown below.

United States plaintiff. (1) Jurisdiction based on 28 U.S.C. 1345 and 1348. Suits by agencies and officers of the United States are included here.

United States defendant. (2) When the plaintiff is suing the United States, its officers or agencies, place an "X" in this box.

Federal question. (3) This refers to suits under 28 U.S.C. 1331, where jurisdiction arises under the Constitution of the United States, an amendment to the Constitution, an act of Congress or a treaty of the United States. In cases where the U.S. is a party, the U.S. plaintiff or defendant code takes precedence, and box 1 or 2 should be marked.

Diversity of citizenship. (4) This refers to suits under 28 U.S.C. 1332, where parties are citizens of different states. When Box 4 is checked, the citizenship of the different parties must be checked. (See Section III below; **NOTE: federal question actions take precedence over diversity cases.**)

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

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

V. Origin. Place an "X" in one of the seven boxes.

Original Proceedings. (1) Cases which originate in the United States district courts.

Removed from State Court. (2) Proceedings initiated in state courts may be removed to the district courts under Title 28 U.S.C., Section 1441.

Remanded from Appellate Court. (3) Check this box for cases remanded to the district court for further action. Use the date of remand as the filing date.

Reinstated or Reopened. (4) Check this box for cases reinstated or reopened in the district court. Use the reopening date as the filing date.

Transferred from Another District. (5) For cases transferred under Title 28 U.S.C. Section 1404(a). Do not use this for within district transfers or multidistrict litigation transfers.

Multidistrict Litigation – Transfer. (6) Check this box when a multidistrict case is transferred into the district under authority of Title 28 U.S.C. Section 1407.

Multidistrict Litigation – Direct File. (8) Check this box when a multidistrict case is filed in the same district as the Master MDL docket.

PLEASE NOTE THAT THERE IS NOT AN ORIGIN CODE 7. Origin Code 7 was used for historical records and is no longer relevant due to changes in statute.

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

VII. Requested in Complaint. Class Action. Place an "X" in this box if you are filing a class action under Rule 23, F.R.Cv.P.

Demand. In this space enter the actual dollar amount being demanded or indicate other demand, such as a preliminary injunction.

Jury Demand. Check the appropriate box to indicate whether or not a jury is being demanded.

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

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

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

DESIGNATION FORM

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

Address of Plaintiff: Marilyn Borne (Walker, LA 70785) and Celia Skorupski (Bristol, CT 06010)

Address of Defendant: Cencora, Inc., 1 West First Avenue, Conshohocken, PA 19428

Place of Accident, Incident or Transaction: Various

RELATED CASE IF ANY:

Case Number: 2:24-cv-02227-CMR Judge: Hon. Cynthia M. Rufe Date Terminated _____

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

1. Is this case related to property included in an earlier numbered suit pending or within one year previously terminated action in this court? Yes No

2. Does this case involve the same issue of fact or grow out of the same transaction as a prior suit Pending or within one year previously terminated action in this court? Yes No

3. Does this case involve the validity or infringement of a patent already in suit or any earlier Numbered case pending or within one year previously terminated action of this court? Yes No

4. Is this case a second or successive habeas corpus, social security appeal, or pro se case filed by the same individual? Yes No

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

DATE: _____ /s/ Jeannine M. Kenney _____ 307635
 Attorney-at-Law *(Must sign above)* Attorney I.D. # (if applicable) _____

Civil (Place a √ in one category only)

A. Federal Question Cases:

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

B. Diversity Jurisdiction Cases:

1. Insurance Contract and Other Contracts
 2. Airplane Personal Injury
 3. Assault, Defamation
 4. Marine Personal Injury
 5. Motor Vehicle Personal Injury
 6. Other Personal Injury (Please specify): _____
 7. Products Liability
 8. All Other Diversity Cases: (Please specify) _____
 Class Action Fairness Act, 28 USC 1332(d)

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

I, Jeannine M. Kenney, counsel of record or pro se plaintiff, do hereby certify:

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

Relief other than monetary damages is sought.

DATE: 06/04/2024

/s/ Jeannine M. Kenney
 Attorney-at-Law *(Sign here if applicable)*

307635
 Attorney ID # (if applicable)

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