UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF PENNSYLVANIA

ROGER WEBB, individually and on behalf of all others similarly situated, Plaintiff, v. CENCORA, INC. and THE LASH GROUP, LLC, Defendants.	Case No. 2:24-cv-2603 **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Plaintiff Roger Webb ("Plaintiff"), individually and on behalf of all others similarly situated, by and through his undersigned attorneys, bring this class action against Cencora, Inc. ("Cencora") and The Lash Group, LLC ("Lash") (together "Defendants") and complain and allege upon personal knowledge as to Plaintiff and upon information and belief as to all other matters.

INTRODUCTION

1. Plaintiff brings this class action against Defendants for their failure to secure and safeguard the personally identifiable information ("PII") and personal health information ("PHI") (collectively, "Personal Information") collected from its customers, their patients, and/or other persons affiliated with Defendants.

2. Defendants are a Conshohocken, Pennsylvania-based pharmaceutical solutions organizations that specializes in pharmaceutical services, including providing drug distribution and solutions for doctor's offices, pharmacies, and animal healthcare.

3. As a condition of receiving Defendants' services, Defendants' customers, patients, and other affiliated persons are required to provide, and entrust, Defendants with sensitive and private information, including PII and PHI.

4. On February 27, 2024, Cencora filed a Form 8-K with the Securities Exchange Commission (SEC) disclosing that it has been impacted by a data breach that resulted in the theft of sensitive information (the "Data Breach"). The SEC filing confirmed that "[o]n February 21, 2024, Cencora learned that data from its information systems had been exfiltrated, some of which may contain personal information." The filing further identified that "[u]pon initial detection of the unauthorized activity, [Cencora] immediately took containment steps and commenced an investigation with the assistance of law enforcement, cybersecurity experts and external counsel."[1]

5. The letter Cencora sent to Plaintiff notifying him about the breach indicates that his impacted information includes names, addresses, dates of birth, diagnosis information, and medication or prescription information, and that Cencora learned of the breach on February 21, 2024; however, it has provided little additional information about the duration or timeline of the breach; no confirmation about the number of individuals impacted; no confirmation about the full universe of the information impacted; and no details about the steps being taken to address and rectify the harms caused by the breach.

6. Cencora's website also provides no mention of or announcement concerning the Data Breach and the steps that Cencora is taking to address it. On information and belief, given the SEC filing made by Cencora and that Cencora collects and maintains highly sensitive Personal Information, the Data Breach impacts many individuals and exposed highly sensitive health and other information.

7. The Data Breach was a direct result of Cencora's failure to implement adequate and reasonable cybersecurity procedures and protocols necessary to protect patients' Personal

[1] Cencora, Inc. (Feb. 27, 2024) *Form 8-K*, available at https://d18rn0p25nwr6d.cloudfront.net/CIK-0001140859/81c828c1-699f-45d0-a610-e985f8e8c4b9.pdf.

Information from the foreseeable threat of a cyberattack.

8. By being entrusted with Plaintiff's and class members' Personal Information for its own pecuniary benefit, Cencora assumed a duty to Plaintiff and class members to implement and maintain reasonable and adequate security measures to secure, protect, and safeguard Plaintiff's and class members' Personal Information against unauthorized access and disclosure.

9. Defendants also had a duty to adequately safeguard this Personal Information under controlling case law, as well as pursuant to industry standards and duties imposed by statutes, including Section 5 of the Federal Trade Commission Act ("FTC Act"). Defendants breached those duties by, among other things, failing to implement and maintain reasonable security procedures and practices to protect patients' Personal Information from unauthorized access and disclosure.

10. As a result of Defendants' inadequate security and breach of their duties and obligations, the Data Breach occurred, and Plaintiff and class members have now had their sensitive Personal Information stolen and exfiltrated, as confirmed by Defendants. Due to the Data Breach, Plaintiff and class members have suffered injury and ascertainable losses in the form of out-of-pocket expenses, loss of value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach, the diminution in value of their Personal Information from its exposure, and the present and imminent threat of fraud and identity theft. This action seeks to remedy these failings and their consequences.

11. Plaintiff's and class members' sensitive and confidential Personal Information remain in the possession of Defendants. Absent additional safeguards and independent review and oversight, the information remains vulnerable to further cyberattacks and theft.

12. Defendants disregarded the rights of Plaintiff and class members by, *inter alia*, failing to take adequate and reasonable measures to ensure its data systems were protected against

unauthorized intrusions; failing to disclose that it did not have adequately robust computer systems and security practices to safeguard its patients' Personal Information; failing to take standard and reasonably available steps to prevent the Data Breach; failing to properly train its staff and employees on proper security measures; and failing to provide Plaintiff and class members prompt and adequate notice of the Data Breach.

13. In addition, Cencora, Lash, and their employees failed to properly monitor the computer network and systems that housed patients' Personal Information. Had Defendants properly and adequately monitored these systems, it would have discovered the intrusion sooner or prevented it altogether.

14. The security of Plaintiff's and class members' identities is now at risk because of Defendants' wrongful conduct as the Personal Information that Defendants collected and maintained is now in the hands of data thieves. This present risk will continue indefinitely.

15. As a result of the Data Breach, Plaintiff and class members have been exposed to a present and imminent risk of fraud and identity theft. Among other measures, Plaintiff and class members must now and in the future closely monitor their financial accounts and medical records to guard against identity theft. Further, Plaintiff and class members will incur out-of-pocket costs to purchase credit monitoring and identity theft protection and insurance services, credit freezes, credit reports, or other protective measures to deter and detect identity theft.

16. Plaintiff and class members will also be forced to expend additional time to review credit reports and monitor their financial accounts and medical records for fraud or identity theft. Moreover, because the exposed information presumably includes health and prescription information, Social Security numbers, and other immutable personal details, the risk of identity theft and fraud will persist throughout their lives.

17. Plaintiff and class members seek to hold Defendants responsible for the harms resulting from the preventable disclosure of such sensitive information. Plaintiff seeks to remedy the harms resulting from the Data Breach individually and on behalf of all similarly situated individuals whose Personal Information was accessed and exfiltrated during the Data Breach.

18. Plaintiff, individually and on behalf of all other class members, brings claims for negligence, negligence per se, breach of fiduciary duty, breach of implied contract, unjust enrichment, breach of confidence, and for declaratory and injunctive relief.

19. To remedy these violations of law, Plaintiff and class members seek actual damages, statutory damages, restitution, and injunctive and declaratory relief (including significant improvements to Defendants' data security protocols and employee training practices), reasonable attorneys' fees, costs, and expenses incurred in bringing this action, and all other remedies this Court deems just and proper.

PARTIES

Plaintiff

20. Plaintiff Roger Webb is a resident and citizen of the state of Tennessee.

21. Plaintiff Webb provided Personal Information to, or otherwise had Personal Information provided to, Cencora in connection with receiving health-related services from Cencora. In obtaining and maintaining Plaintiff's Personal Information for its business purposes, Cencora expressly and impliedly promised, and undertook a duty, to act reasonably in its handling of Plaintiff's Personal Information. Cencora, however, did not take proper care of Plaintiff's Personal Information, leading, on information and belief, to its exposure to and exfiltration by cybercriminals as a direct result of Cencora's inadequate security measures.

22. On or about May 17, 2024, Cencora sent, and Plaintiff received, a letter notifying

Plaintiff that his Personal Information was exposed in the Data Breach.

23. Once Personal Information is exposed, there is virtually no way to ensure that the exposed information has been fully recovered or contained against future misuse. For this reason, Plaintiff will need to maintain these heightened measures for years.

24. Plaintiff also suffered actual injury from having Personal Information compromised as a result of the Data Breach, including, but not limited to: (a) damage to and diminution in the value of Plaintiff's confidential Personal Information—a form of property that Plaintiff entrusted to Cencora, which was compromised as a result of the Data Breach it failed to prevent; and (b) a violation of Plaintiff's privacy rights as a result of Cencora's unauthorized disclosure of Plaintiff's Personal Information.

25. Had Plaintiff known that Cencora does not adequately protect Personal Information, Plaintiff would not have used Cencora's services and/or agreed to allow Cencora to receive and maintain Plaintiff's Personal Information.

26. As a result of Cencora's failure to adequately safeguard Plaintiff's information, Plaintiff has been injured. Plaintiff is also at a continued risk of harm because the Personal Information remains in Cencora's systems, which have already been shown to be susceptible to compromise and attack and is subject to further attack so long as Cencora fails to undertake the necessary and appropriate data security measures to protect the PII and PHI in its possession.

Defendants

27. Defendant Cencora, Inc. is a corporation organized under the laws of the state of Delaware, with a principal place of business located at 1 West First Avenue, Conshohocken, Pennsylvania 19428.

28. Defendant the Lash Group, LLC is a company with its principal place of business located at 1 West 1st Avenue, Conshohocken, PA 19428.

JURISDICTION AND VENUE

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

30. This Court has personal jurisdiction over Cencora because Cencora maintains its principal place of business in this District and conducts substantial business in Pennsylvania and in this District through its principal place of business; engaged in the conduct at issue herein from and within this District; and otherwise has substantial contacts with this District and purposely availed itself of the Courts in this District.

31. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(b)(1) and (2) because Cencora resides in this District, and this District is where a substantial part of the acts, omissions, and events giving rise to Plaintiff's claims occurred.

FACTUAL ALLEGATIONS

A. Overview of Defendants

32. Cencora, Inc. is one of the largest global pharmaceutical sourcing and distribution services companies.[2] In August of 2023, Cencora announced the completion of its name and stock ticker change from AmerisourceBergen Corporation.[3]

---

[2] Cencora, Inc. (2023). *Form 10-K 2023*. Cencora, Inc., available at https://investor.cencora.com/files/doc_financials/2023/ar/Cencora-FY2023-10-K-Web-Posting.pdf.

[3] *AmerisourceBergen becomes Cencora, in alignment with the company's growing global footprint and central role in pharmaceutical access and care*, CENCORA (Aug. 30, 2022), https://www.cencora.com/newsroom/press-releases/amerisourcebergen-becomes-cencora.

33. "The new name underscores Cencora's experience and vision when it comes to connecting manufacturers, providers, pharmacies and patients, and ensuring the consistent, reliable flow of treatments to those who need them at a time of growing complexity," the company explained in a press release. "Our new name is a reminder of our customers, their patients, and our team members who are at the center of everything we do," said Steven H. Collis, Chairman, President & Chief Executive Officer of Cencora, in the release.[4]

34. To date, Cencora has more than 46,000 employees and is ranked #11 on the Fortune 500 and #24 on the Global Fortune 500, with over $230 billion in annual revenue.[5]

35. Cencora offers a broad range of services to its customers—including healthcare providers and pharmaceutical and biotech manufacturers—through a geographically diverse network of distribution service centers and other operations in the United States and select global markets.[6]

36. Specifically, Cencora distributes "a comprehensive offering of brand-name, specialty brand-name, and generic pharmaceuticals, over-the-counter healthcare products, home healthcare supplies and equipment, and related services to a wide variety of healthcare providers located in the United States and select global markets, including acute care hospitals and health systems, independent and chain retail pharmacies, mail order pharmacies, medical clinics, long-term care and alternate site pharmacies, physician practices, medical and dialysis clinics, veterinarians, and other customers."[7]

---

[4] *Id.*
[5] *Cencora Reports Fiscal 2024 First Quarter Results*, CENCORA (JAN. 31, 2024), https://investor.cencora.com/news/news-details/2024/Cencora-Reports-Fiscal-2024-First-Quarter-Results/default.aspx.
[6] Cencora, Inc. *Form 10-K 2023*, *supra*, n.2.
[7] *Id.*

37. Additionally, Cencora offers "healthcare providers and pharmaceutical manufacturers with an assortment of related services, including data analytics, outcomes research, reimbursement and pharmaceutical consulting services (including regulatory affairs, development consulting and scientific affairs, pharmacovigilance, and quality management and compliance) niche premium logistics services, inventory management, pharmacy automation, pharmacy management, and packaging solutions."[8]

38. Lash is a patient support company, owned by Defendant Cencora, that provides patient support services, business analytics and technology services, and other services to pharmaceutical companies, pharmacies, and other healthcare providers.[9]

39. In the regular course of their business, Defendants collect and maintain PII/PHI from customers, patients, and other affiliated persons, including those to whom they are currently providing or previously provided healthcare services, pharmaceutical services and/or other related services.[10]

40. As a regular part of their business, Defendants require customers, patients, and other affiliated persons, to provide Personal Information before providing them services. On information and belief, that information includes, but is not limited to: personally identifiable information (such as names, postal addresses, email addresses, telephone numbers, or other similar identifiers); financial information (such as routing numbers, account numbers, billing addresses, records of payment, and other payment information); and highly sensitive personal information (such as SSNs, driver's license, state identification card, and/or passport numbers, precise geolocation, racial or ethnic origin, genetic data, the processing of biometric information for the

[8] *Id.*
[9] https://www.lashgroup.com/ (last accessed June 11, 2024).
[10] *See Privacy Statement*, CENCORA (Aug. 30, 2023), https://www.cencora.com/global-privacy-statement (last accessed June 11, 2024).

purpose of uniquely identifying a consumer, personal information collected and analyzed concerning an individual's health, and personal information collected and analyzed concerning an individual's sex life or sexual orientation).[11] Cencora stores this information digitally.

41. In its "Global Privacy Statement Overview," available on Cencora's website, Cencora affirms that it "value[s] and protect the personal information entrusted to the company by its suppliers, customers, and visitors."[12] Cencora states that "[a]s 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."[13]

42. In its Privacy Statement, also available on Cencora's website, Cencora states that it "may collect Personal [Information] directly from you when you visit our Websites, choose to use services or participate in programs or otherwise provide Personal [Information] directly to us."[14] Cencora further states that it "use[s] appropriate technical, administrative and physical safeguards to protect Personal [Information] from loss, misuse or alteration."[15]

43. Plaintiff and class members are, or were, patients and customers of or otherwise affiliated with Cencora and/or received healthcare, pharmaceutical or other related services from Cencora, or otherwise are affiliated or transacted with Cencora, and entrusted Cencora with their PII/PHI or otherwise had their PII/PHI entrusted to Cencora.

---

[11] *Id.*; *see, e.g.*, *State Supplement to Privacy Statement*, CENCORA, https://www.cencora.com/global-california-supplement (last accessed June 11, 2024); *Applicant Privacy Statement*, CENCORA, https://www.cencora.com/Global-Applicant-Privacy-Statement (last accessed June 11, 2024).
[12] *Privacy Statement*, *supra*, n.10.
[13] *Id.*
[14] *Id.*
[15] *Id.*

B. The Data Breach Compromised Plaintiff's and Class Members' PII/PHI

44. On February 27, 2024, Cencora filed a Form 8-K with the SEC disclosing that it has been impacted by a data breach that resulted in the theft of sensitive information (the "Data Breach"). The SEC filing confirmed that "[o]n February 21, 2024, Cencora learned that data from its information systems had been exfiltrated, some of which may contain personal information." The filing further identified that "[u]pon initial detection of the unauthorized activity, [Cencora] immediately took containment steps and commenced an investigation with the assistance of law enforcement, cybersecurity experts and external counsel."[16]

45. Cencora has provided no additional information about the Data Breach, leaving class members in the dark about the details of the breach, the nature of the information impacted, and what they could be doing to protect themselves from fraud and identity theft.

46. Cencora's website also provides no mention of or announcement concerning the Data Breach and the steps that Cencora is taking to address it. On information and belief, given the SEC filing made by Cencora and that Cencora collects and maintains highly sensitive Personal Information, the Data Breach impacts many individuals and exposed sensitive information such as health insurance information, health information, Social Security numbers, prescription information, and other medical information.

47. Cencora's Form 8-K filing omits pertinent information including how criminals gained access to the encrypted files on its systems, what computer systems were impacted, the means and mechanisms of the cyberattack, the reason for the two-month delay in notifying Plaintiff and class members of the Data Breach, how it determined that the Personal Information had been accessed, and of particular importance to Plaintiff and class members, what actual steps Cencora

[16] Cencora, Inc. (Feb. 27, 2024) *Form 8-K*, n.1, *supra*.

took following the Data Breach to secure its systems and train its employees to prevent further cyberattacks.

48. Based on Cencora's acknowledgment that Personal Information was "exfiltrated" by an unauthorized party, it is evident that unauthorized criminal actors did in fact access Cencora's network and steal Plaintiff's and class members' Personal Information in an attack designed to acquire the sensitive, confidential, and valuable information.

49. The Personal Information contained in the files accessed by cybercriminals presumably was not encrypted because if properly encrypted, the attackers would have acquired unintelligible data and would not have "accessed" Personal Information.

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

51. The targeted attack was expressly designed to gain access to and exfiltrate private and confidential data, including (among other things) the Personal Information of patients, such as Plaintiff and class members.

52. Due to Cencora's inadequate security measures, Plaintiff and class members now face a present, immediate, and ongoing risk of fraud and identity theft and must deal with that threat forever.

53. Cencora was obligated to Plaintiff and class members to keep their Personal Information confidential and to protect it from unauthorized access and disclosure.

54. Plaintiff and class members entrusted their Personal Information to Cencora with the reasonable expectation and mutual understanding that Cencora or anyone who used their Personal Information in conjunction with the health or pharmaceutical services they received

would comply with obligations to keep such information confidential and secure from unauthorized access after it received such information.

55. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and class members' Personal Information, Cencora assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiff's and class members' Personal Information from unauthorized disclosure.

56. Plaintiff and the class members have taken reasonable steps to maintain the confidentiality of their personal information. Plaintiff and class members would not have allowed Cencora or anyone in Cencora's position to receive their PII/PHI had they known that Cencora would fail to implement industry standard protections for that sensitive information.

57. As a result of Cencora's conduct, Plaintiff's and class members' highly confidential and sensitive Personal Information was left exposed to cybercriminals.

C. Cencora Failed to Follow FTC Guidelines

58. Cencora was also prohibited by the Federal Trade Commission Act (the "FTC Act") (15 U.S.C. § 45) from engaging in "unfair or deceptive acts or practices in or affecting commerce." The Federal Trade Commission (the "FTC") has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of the FTC Act. *See, e.g., FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015).

59. The FTC has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices.

60. According to the FTC, the need for data security should be factored into all business decision-making.

61. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cyber-security guidelines for businesses.

62. The guidelines note that businesses should protect the personal patient information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.

63. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.

64. The FTC further recommends that companies not maintain private information longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

65. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect patient data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

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

67. Cencora's failure to employ reasonable and appropriate measures to protect against unauthorized access to the Personal Information in its possession, constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

68. Cencora was at all times fully aware of its obligation to protect the Personal Information in its possession. Cencora was also aware of the significant repercussions that would result from its failure to do so.

D. Cencora Failed to Comply with Industry Standards

69. As described above, experts studying cyber security routinely identify healthcare providers and their business associates as being particularly vulnerable to cyberattacks because of the value of the PII and PHI which they collect and maintain.

70. Several best practices have been identified that at a minimum should be implemented by entities like Cencora, including but not limited to: educating 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; and limiting which employees can access sensitive data.

71. Other best cyber-security practices that are standard in the healthcare industry include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches, and routers; monitoring and protection of physical security systems; protection against any possible communication system; and training staff regarding critical points.

72. Cencora 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.

73. The foregoing frameworks are existing and applicable industry standards in the healthcare industry, and Cencora failed to comply with these accepted standards, thereby opening the door to cybercriminals and causing the Data Breach.

E. Cencora Owed Plaintiff and Class Members a Duty to Safeguard Their Personal Information

74. In addition to its obligations under federal and state laws, Cencora owed a duty to Plaintiff and class members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the Personal Information in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. Cencora owed a duty to Plaintiff and class members to provide reasonable security, including consistency with industry standards and requirements, and to ensure that its computer systems, networks, and protocols adequately protected the Personal Information of class members.

75. Cencora owed a duty to Plaintiff and class members to create and implement reasonable data security practices and procedures to protect the Personal Information in its possession, including adequately training its employees and others who accessed private information within its computer systems on how to adequately protect Private Information.

76. Cencora owed a duty to Plaintiff and class members to implement processes that would detect a compromise of Personal Information in a timely manner.

77. Cencora owed a duty to Plaintiff and class members to act upon data security warnings and alerts in a timely fashion.

78. Cencora owed a duty to Plaintiff and class members to disclose in a timely and

accurate manner when and how the Data Breach occurred.

79. Cencora owed a duty of care to Plaintiff and class members because they were foreseeable and probable victims of any inadequate data security practices.

F. Cencora Knew That Criminals Target PII/PHI

80. Cencora's data security obligations were particularly important given the substantial increase in cyberattacks and/or data breaches in the healthcare industry and other industries holding significant amounts of PII and PHI preceding the date of the breach.

81. At all relevant times, Cencora knew, or should have known, its patients', Plaintiff's, and all other class members' PII/PHI was a target for malicious actors. Despite such knowledge, Cencora failed to implement and maintain reasonable and appropriate data privacy and security measures to protect Plaintiff's and class members' Personal Information from cyber-attacks that Cencora should have anticipated and guarded against.

82. The targeted attack was expressly designed to gain access to and exfiltrate private and confidential data, including (among other things) the Personal Information Cencora collects from its customers, their patients and/or other affiliated persons, like Plaintiff and class members.

83. Cybercriminals seek out PHI at a greater rate than other sources of personal information. In a 2022 report, the healthcare compliance company Proetus found that there were 905 medical data breaches in 2021, leaving over 50 million patient records exposed for 700 of the 2021 incidents. This is an increase from the 758 medical breaches Protenus compiled in 2020.[17]

84. The healthcare sector suffered about 337 breaches in the first half of 2022 alone, according to Fortified Health Security's mid-year report released in July. The percentage of healthcare breaches attributed to malicious activity rose more than 5 percentage points in the first

[17] *2022 Breach Barometer*, Protenus (2022), https://www.protenus.com/breach-barometer-report.

six months of 2022 to account for nearly 80 percent of all reported incidents.[18]

85. Further, a 2022 report released by IBM Security states that for 12 consecutive years the healthcare industry has had the highest average cost of a data breach and as of 2022 healthcare data breach costs have hit a new record high.[19]

86. Personal Information is a valuable property right.[20] The value of Personal Information as a commodity is measurable.[21] "Firms are now able to attain significant market valuations by employing business models predicated on the successful use of personal data within the existing legal and regulatory frameworks."[22] American companies are estimated to have spent over $19 billion on acquiring personal data of consumers in 2018.[23] It is so valuable to identity thieves that once Personal Information has been disclosed, criminals often trade it on the "cyber black-market," or the "dark web," for many years.

87. As a result of its real value and the recent large-scale data breaches, identity thieves and cybercriminals have openly posted credit card numbers, Social Security numbers, Personal Information, and other sensitive information directly on various internet websites, making the

---

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

[19] *Cost of a Data Breach Report 2022*, IBM Security (July 2022), https://www.ibm.com/downloads/cas/3R8N1DZJ.

[20] *See* Marc van Lieshout, *The Value of Personal Data*, 457 IFIP Advances in Information and Communication Technology (May 2015), https://www.researchgate.net/publication/283668023 ("The value of [personal] information is well understood by marketers who try to collect as much data about personal conducts and preferences as possible...").

[21] *See* Robert Lowes, *Stolen EHR [Electronic Health Record] Charts Sell for $50 Each on Black Market*, Medscape (Apr. 28, 2014), http://www.medscape.com/viewarticle/824192.

[22] *Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value*, OECD Digital Economy Papers, No. 220, OECD Publishing (Apr. 2, 2013), https://www.oecd-ilibrary.org/science-and-technology/exploring-the-economics-of-personal-data_5k486qtxldmq-en.

[23] *U.S. Firms to Spend Nearly $19.2 Billion on Third-Party Audience Data and Data-Use Solutions in 2018, Up 17.5% from 2017*, Interactive Advertising Bureau (Dec. 5, 2018), https://www.iab.com/news/2018-state-of-data-report/.

information publicly available. This information from various breaches, including the information exposed in the Data Breach, can be aggregated and become more valuable to thieves and more damaging to victims.

88. PHI is particularly valuable and has been referred to as a "treasure trove for criminals."[24] A cybercriminal who steals a person's PHI can end up with as many as "seven to 10 personal identifying characteristics of an individual."[25] A study by Experian found that the "average total cost" of medical identity theft is "about $20,000" per incident, 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.[26]

89. Personal information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[27] Experian reports that a stolen credit or debit card number can sell for $5 to $110 on the dark web.[28] All-inclusive health insurance dossiers containing sensitive health insurance information, names, addresses, telephone numbers, email addresses, Social Security numbers, and bank account information, complete with account and routing numbers, can fetch up to $1,200 to $1,300 each on the black market.[29] Criminals can also

[24] *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.").
[25] *Id.*
[26] Elinor Mills, *Study: Medical identity theft is costly for victims*, CNET (Mar. 3, 2010), https://www.cnet.com/news/study-medical-identity-theft-is-costly-for-victims.
[27] Anita George, *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends (Oct. 16, 2019), https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/.
[28] Brian Stack, *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian (Dec. 6, 2017), https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/.
[29] Adam Greenberg, *Health insurance credentials fetch high prices in the online black market*, SC Magazine (July 16, 2013), https://www.scmagazine.com/news/breach/health-insurance-credentials-fetch-high-prices-in-the-online-black-market.

purchase access to entire company data breaches from $900 to $4,500.[30] According to a report released by the Federal Bureau of Investigation's ("FBI") Cyber Division, criminals can sell healthcare records for 50 times the price of a stolen Social Security or credit card number.[31]

90. Criminals can use stolen Personal Information to extort a financial payment by "leveraging details specific to a disease or terminal illness."[32] Quoting Carbon Black's Chief Cybersecurity Officer, one recent article explained: "Traditional criminals understand the power of coercion and extortion . . . . By having healthcare information—specifically, regarding a sexually transmitted disease or terminal illness—that information can be used to extort or coerce someone to do what you want them to do."[33]

91. Consumers place a high value on the privacy of that data. Researchers shed light on how much consumers value their data privacy—and the amount is considerable. Indeed, studies confirm that "when privacy information is made more salient and accessible, some consumers are willing to pay a premium to purchase from privacy protective websites."[34]

92. Given these facts, any company that transacts business with a consumer and then compromises the privacy of consumers' Personal Information has thus deprived that consumer of the full monetary value of the consumer's transaction with the company.

93. Indeed, cyberattacks against the healthcare industry have been common for over 10 years, with the FBI warning as early as 2011 that cybercriminals were "advancing their abilities to

---

[30] *In the Dark*, VPNOverview.com, https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last accessed on Feb. 29, 2024).
[31] *See Health Care Systems and Medical Devices at Risk for Increased Cyber Intrusions for Financial Gain*, FBI Cyber Division (Apr. 8, 2014), https://www.illuminweb.com/wp-content/uploads/ill-mo-uploads/103/2418/health-systems-cyber-intrusions.pdf.
[32] *See What Happens to Stolen Healthcare Data?*, n.24, *supra*.
[33] *Id.*
[34] Janice Y. Tsai et al., *The Effect of Online Privacy Information on Purchasing Behavior, An Experimental Study*, 22(2) Information Systems Research 254 (June 2011), https://www.jstor.org/stable/23015560?seq=1.

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 that "the increasing sophistication of cyber criminals will no doubt lead to an escalation in cybercrime."[35]

94. Cyberattacks have become so notorious that the FBI and U.S. Secret Service have 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 to ransomware criminals … because they often have lesser IT defenses and a high incentive to regain access to their data quickly."[36]

95. In fact, according to the cybersecurity firm Mimecast, 90% of healthcare organizations experienced cyberattacks in the past year.[37]

96. Cencora was on notice that the FBI has recently been concerned about data security in the healthcare industry. In August of 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)."[38]

---

[35] 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.

[36] Ben Kochman, *FBI, Secret Service Warn of Targeted Ransomware*, Law360 (Nov. 18, 2019), https://www.law360.com/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware.

[37] *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.

[38] Jim Finkle, *FBI Warns Healthcare Firms that they are Targeted by Hackers*, Reuters (Aug. 2014), https://www.reuters.com/article/us-cybersecurity-healthcare-fbi/fbi-warns-healthcare-firms-they-are-targeted-by-hackers-idUSKBN0GK24U20140820.

97. 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.[39]

98. As implied by the above AMA quote, stolen Personal Information can be used to interrupt important medical services. This is an imminent and certainly impending risk for Plaintiff and class members.

99. Cencora was on notice that the federal government has been concerned about healthcare company data encryption practices. Cencora knew its employees accessed and utilized protected health information in the regular course of their duties, yet it appears that information was not encrypted.

100. The Office for Civil Rights ("OCR") urges the use of encryption of data containing sensitive personal information. As long ago 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, OCR's deputy director of health information privacy, stated "[o]ur message to these organizations is simple: encryption is your best defense against these incidents."[40]

---

[39] Andis Robeznieks, *Cybersecurity: Ransomware attacks shut down clinics, hospitals*, American Medical Association (Oct. 4, 2019), https://www.ama-assn.org/practice-management/sustainability/cybersecurity-ransomware-attacks-shut-down-clinics-hospitals.

[40] *Stolen Laptops Lead to Important HIPAA Settlements*, U.S. Department of Health and Human Services (Apr. 22, 2014), https://wayback.archive-it.org/3926/20170127085330/https://www.hhs.gov/about/news/2014/04/22/stolen-laptops-lead-to-important-hipaa-settlements.html.

101. Cencora knew or should have known about its data security vulnerabilities and implemented enhanced and adequate protection, particularly given the nature of the Personal Information stored in its unprotected files.

G. Theft of PII/PHI Has Grave and Lasting Consequences for Victims

102. Theft of PII/PHI is serious. The FTC warns consumers that identity thieves use PII/PHI to exhaust financial accounts, receive medical treatment, start new utility accounts, and incur charges and credit in a person's name.[41]

103. Identity thieves use personal information for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.[42] According to Experian, one of the largest credit reporting companies in the world, "[t]he research shows that personal information is valuable to identity thieves, and if they can get access to it, they will use it" to among other things: open a new credit card or loan, change a billing address so the victim no longer receives bills, open new utilities, obtain a mobile phone, open a bank account and write bad checks, use a debit card number to withdraw funds, obtain a new driver's license or ID, and/or use the victim's information in the event of arrest or court action.[43]

---

[41] *See What to Know About Identity Theft*, Federal Trade Commission Consumer Advice, https://www.consumer.ftc.gov/articles/what-know-about-identity-theft (last accessed on June 11, 2024).

[42] The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 12 C.F.R. § 1022.3(h). The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, social security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number." 12 C.F.R. § 1022.3(g).

[43] Susan Henson, *What Can Identity Thieves Do with Your Personal Information and How Can You Protect Yourself?*, Experian (Sept. 1, 2017), https://www.experian.com/blogs/ask-experian/what-can-identity-thieves-do-with-your-personal-information-and-how-can-you-protect-yourself/.

104. With access to an individual's Personal Information, criminals can do more than just empty a victim's bank account—they can also commit all manner of fraud, including: obtaining a driver's license or official identification card in the victim's name but with the thief's picture, using the victim's name and Social Security number to obtain government benefits, or filing a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's Social Security number, rent a house, or receive medical services in the victim's name, and may even give the victim's personal information to police during an arrest, resulting in an arrest warrant being issued in the victim's name.[44]

105. Each year, identity theft causes tens of billions of dollars of losses to victims in the United States. For example, with the Personal Information stolen in the Data Breach, which includes Social Security numbers, identity thieves can open financial accounts, commit medical fraud, apply for credit, file fraudulent tax returns, commit crimes, create false driver's licenses and other forms of identification and sell them to other criminals or undocumented immigrants, steal government benefits, give breach victims' names to police during arrests, and many other harmful forms of identity theft. These criminal activities have and will result in devastating financial and personal losses to Plaintiff and class members.

106. Personal Information is such a valuable commodity to identity thieves that once it has been compromised, criminals will use it and trade the information on dark web black markets for years.

107. For example, it is believed that certain highly sensitive Personal Information compromised in the 2017 Experian data breach was being used, three years later, by identity thieves to apply for COVID-19-related unemployment benefits.

---

[44] *See Warning Signs of Identity Theft*, Federal Trade Commission, https://www.identitytheft.gov/Warning-Signs-of-Identity-Theft (last accessed June 11, 2024).

108. The Personal Information exposed in this Data Breach is valuable to identity thieves for use in the kinds of criminal activity described herein. These risks are both certainly impending and substantial. As the FTC has reported, if cyber thieves get access to a person's highly sensitive information, they will use it.[45]

109. Cyber criminals may not use the information right away. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

> [I]n 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.[46]

110. For instance, with a stolen Social Security number, which is only one subset of the Personal Information compromised in the Data Breach, someone can open financial accounts, get medical care, file fraudulent tax returns, commit crimes, and steal benefits.[47]

111. Identity thieves can use Social Security numbers to obtain a driver's license or official identification card in the victim's name but with the thief's picture; use the victim's name and Social Security number to obtain government benefits; or file a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's Social Security number, rent a house or receive medical services in the victim's name, and may even give

---

[45] Ari Lazarus, *How fast will identity thieves use stolen info?*, Federal Trade Commission (May 24, 2017), https://www.consumer.ftc.gov/blog/2017/05/how-fast-will-identity-thieves-use-stolen-info.

[46] *Report to Congressional Requesters: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, United States Government Accountability Office, https://www.gao.gov/assets/gao-07-737.pdf.

[47] *See, e.g.*, Christine DiGangi, *5 Ways an Identity Thief Can Use Your Social Security Number*, USATODAY (Nov. 15, 2017), https://www.usatoday.com/story/money/personalfinance/2017/11/15/5-ways-identity-thief-can-use-your-social-security-number/860643001/ .

the victim's Personal Information to police during an arrest resulting in an arrest warrant being issued in the victim's name.

112. This data demands a much higher price on the black market. Martin Walter, senior director at the cybersecurity firm RedSeal, explained, "[c]ompared to credit card information, personally identifiable information and Social Security [n]umbers are worth more than 10x on the black market."

113. Identity theft is not an easy problem to solve. In a survey, the Identity Theft Resource Center found that most victims of identity crimes need more than a month to resolve issues stemming from identity theft and some need over a year.[48]

114. Theft of Social Security numbers also creates a particularly alarming situation for victims because those numbers cannot easily be replaced. In order to obtain a new number, a breach victim has to demonstrate ongoing harm from misuse of his or her Social Security number, and a new Social Security number will not be provided until after the victim has suffered the harm.

115. Due to the highly sensitive nature of Social Security numbers, theft of Social Security numbers in combination with other PII (e.g., name, address, date of birth) is akin to having a master key to the gates of fraudulent activity. TIME quotes data security researcher Tom Stickley, who is employed by companies to find flaws in their computer systems, as stating, "If I have your name and your Social Security number and you haven't gotten a credit freeze yet, you're easy pickings."[49]

116. Theft of Personal Information is even more serious when it includes theft of PHI.

---

[48] *2021 Consumer Aftermath Report: How Identity Crimes Impact Victims, their Families, Friends, and Workplaces*, Identity Theft Resource Center (2021), https://www.idtheftcenter.org/identity-theft-aftermath-study/.

[49] Patrick Lucas Austin, *'It Is Absurd.' Data Breaches Show it's Time to Rethink How We Use Social Security Numbers, Experts Say*, TIME (Aug. 5, 2019), https://time.com/5643643/capital-one-equifax-data-breach-social-security/.

Medical identity theft is one of the most common, most expensive, and most difficult-to-prevent forms of identity theft. According to Kaiser Health News, "medical-related identity theft accounted for 43 percent of all identity thefts reported in the United States in 2013," which is more than identity thefts involving banking and finance, the government and the military, or education.[50] "Medical identity theft is a growing and dangerous crime that leaves its victims with little to no recourse for recovery," reported Pam Dixon, executive director of World Privacy Forum. "Victims often experience financial repercussions and worse yet, they frequently discover erroneous information has been added to their personal medical files due to the thief's activities."[51]

117. Data breaches involving medical information "typically leave[] a trail of falsified information in medical records that can plague victims' medical and financial lives for years."[52] It "is also more difficult to detect, taking almost twice as long as normal identity theft."[53] In warning consumers on the dangers of medical identity theft, the FTC states that an identity thief may use Personal Information "to see a doctor, get prescription drugs, buy medical devices, submit claims with your insurance provider, or get other medical care."[54] The FTC also warns, "If the thief's health information is mixed with yours, it could affect the medical care you're able to get or the health insurance benefits you're able to use. It could also hurt your credit."[55]

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

---

[50] Michael Ollove, *The Rise of Medical Identity Theft in Healthcare*, KAISER HEALTH NEWS (Feb. 7, 2014), https://khn.org/news/rise-of-indentity-theft/.
[51] *Id.*
[52] Pam Dixon and John Emerson, *The Geography of Medical Identity Theft*, WORLD PRIVACY FORUM (Dec. 12, 2017), https://www.worldprivacyforum.org/2017/12/new-report-the-geography-of-medical-identity-theft/.
[53] *See Health Care Systems and Medical Devices at Risk for Increased Cyber Intrusions for Financial Gain*, n.31, *supra*.
[54] *See What to Know About Identity Theft*, n.41, *supra*.
[55] *Id.*

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

- Significant bills for medical goods and services not sought nor received.

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

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

- Serious life consequences resulting from the crime; for example, victims have been falsely accused of being drug users based on falsified entries to their medical files; victims have had their children removed from them due to medical activities of the imposter; victims have been denied jobs due to incorrect information placed in their health files due to the crime.

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

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

- Sales of medical debt arising from identity theft can perpetuate a victim's debt collection and credit problems, through no fault of their own.[56]

119. There may also be a time lag between when sensitive Personal Information is stolen, when it is used, and when a person discovers it has been used. Fraud and identity theft resulting from the Data Breach may go undetected until debt collection calls commence months, or even years, later. An individual may not know that his or her Social Security number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

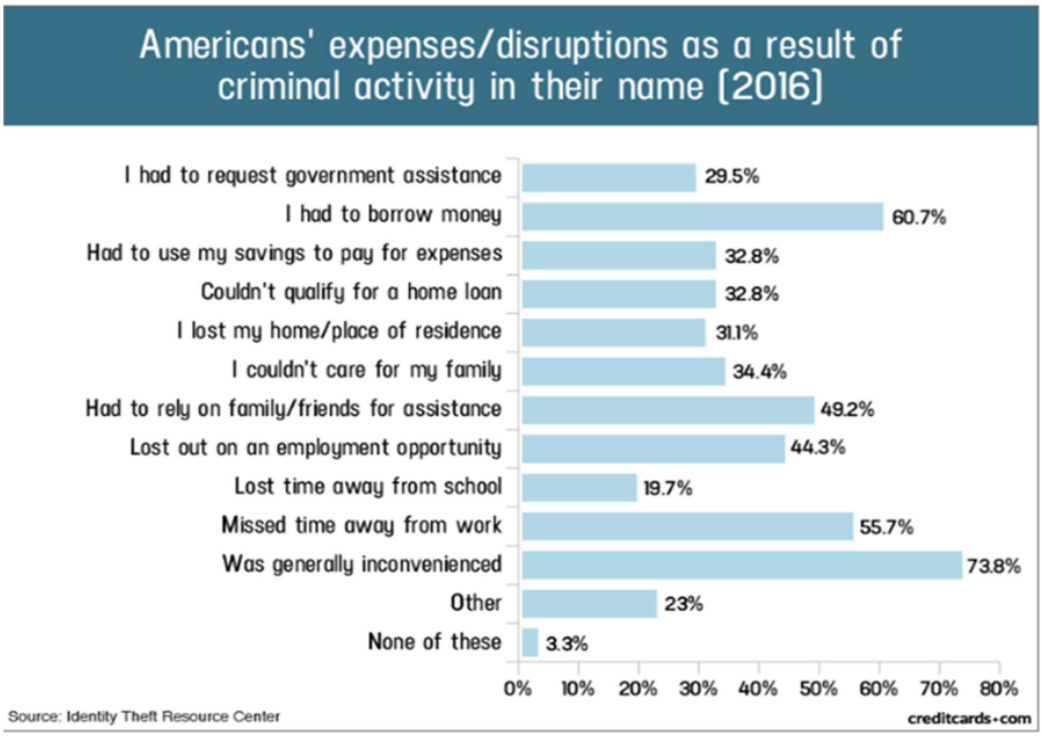
120. For example, on average it takes approximately three months for consumers to discover their identity has been stolen and used, and it takes some individuals up to three years to

[56] *See The Geography of Medical Identity Theft*, n.52, *supra*.

learn that information.[57]

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

122. A study by the Identity Theft Resource Center shows the multitude of harms caused by fraudulent use of personal and financial information:



123. Victims of the Data Breach, like Plaintiff and class members, must spend many hours and large amounts of money protecting themselves from the current and future negative impacts to their privacy and credit because of the Data Breach.[58]

[57] John W. Coffey, *Difficulties in Determining Data Breach Impacts*, 17 Journal of Systemics, Cybernetics and Informatics 9 (2019), http://www.iiisci.org/journal/pdv/sci/pdfs/IP069LL19.pdf.
[58] *Guide for Assisting Identity Theft Victims*, FEDERAL TRADE COMMISSION, 4 (Sept. 2013), http://www.global-screeningsolutions.com/Guide-for-Assisting-ID-Theft-Victims.pdf.

124. As a direct and proximate result of the Data Breach, Plaintiff and class members have been placed at an imminent, immediate, and continuing increased risk of harm from fraud and identity theft. Plaintiff and class members must now take the time and effort (and spend the money) to mitigate the actual and potential impact of the Data Breach on their everyday lives, including purchasing identity theft and credit monitoring services every year for the rest of their lives, placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions and healthcare providers, closing or modifying financial accounts, and closely reviewing and monitoring bank accounts, credit reports, and health insurance account information for unauthorized activity for years to come.

125. Plaintiff and class members have suffered or will suffer actual harms for which they are entitled to compensation, including but not limited to the following:

a. Trespass, damage to, and theft of their personal property, including Private Information;

b. Improper disclosure of their Personal Information;

c. The imminent and certainly impending injury flowing from actual and potential future fraud and identity theft posed by their Personal Information being in the hands of criminals and having already been misused;

d. The imminent and certainly impending risk of having their confidential medical information used against them by spam callers to defraud them;

e. Damages flowing from Defendant's untimely and inadequate notification of the Data Breach;

f. Loss of privacy suffered as a result of the Data Breach;

g. Ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably expended to remedy or mitigate the effects of the data breach;

h. Ascertainable losses in the form of deprivation of the value of patients' personal information for which there is a well-established and quantifiable national and international market;

i. The loss of use of and access to their credit, accounts, and/or funds;

j. Damage to their credit due to fraudulent use of their Private Information; and

k. Increased cost of borrowing, insurance, deposits, and other items which are adversely affected by a reduced credit score.

126. Moreover, Plaintiff and class members have an interest in ensuring that their Personal Information, which remains in the possession of Defendant, is protected from further public disclosure by the implementation of better employee training and industry standard and statutorily compliant security measures and safeguards. Defendants have shown themselves to be wholly incapable of protecting Plaintiff's and class members' Personal Information.

127. Because of the value of its collected and stored data, the medical industry has experienced disproportionally higher numbers of data theft events than other industries. For this reason, Defendants knew or should have known about these dangers and strengthened its data security accordingly. Defendants were put on notice of the substantial and foreseeable risk of harm from a data breach, yet it failed to properly prepare for that risk.

H. The Data Breach Was Foreseeable and Preventable

128. Data disclosures and data breaches are preventable.[59] As Lucy Thompson wrote in the Data Breach and Encryption Handbook, "[i]n almost all cases, the data breaches that occurred

[59] Lucy L. Thompson, *Despite the Alarming Trends, Data Breaches Are Preventable*, Data Breach and Encryption Handbook (Lucy Thompson, ed., 2012).

could have been prevented by proper planning and the correct design and implementation of appropriate security solutions."[60] She added that "[o]rganizations that collect, use, store, and share sensitive personal data must accept responsibility for protecting the information and ensuring that it is not compromised . . . ."[61]

129. "Most of the reported data breaches are a result of lax security and the failure to create or enforce appropriate security policies, rules, and procedures … Appropriate information security controls, including encryption, must be implemented and enforced in a rigorous and disciplined manner so that a *data breach never occurs*."[62]

130. As explained by the Federal Bureau of Investigation, "[p]revention is the most effective defense against ransomware and it is critical to take precautions for protection."[63]

131. Plaintiff and class members entrusted their Personal Information to Defendants as a condition of receiving healthcare-related services. Plaintiff and class members understood and expected that Defendants or anyone in Defendants' position would safeguard their Personal Information against cyberattacks, delete or destroy Personal Information that Defendants were no longer required to maintain, and timely and accurately notify them if their Personal Information was compromised.

I. Plaintiff's and Class Members' Damages

132. To date, Defendants' have done nothing to provide Plaintiff and class members with relief for the damages they have suffered as a result of the Data Breach.

---

[60] *Id.* at 17.
[61] *Id.* at 28.
[62] *Id.*
[63] *See How to Protect Your Networks from RANSOMWARE*, at 3, FBI.GOV, https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view (last accessed June 11, 2024).

133. Plaintiff and class members have been damaged by the compromise of their Personal Information in the Data Breach.

134. As a direct and proximate result of Defendants' conduct, Plaintiff and class members have been placed at an imminent, immediate, and continuing increased risk of harm from fraud and identity theft. Plaintiff 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.

135. Plaintiff and class members face substantial risk of being targeted for future phishing, data intrusion, and other illegal schemes based on their Personal Information, as potential fraudsters could use that information to target such schemes more effectively to Plaintiff and class members.

136. Plaintiff and class members have and will 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.

137. Plaintiff 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 financial and other 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 numbers, medical insurance accounts, bank accounts, and credit reports for unauthorized activity for years to come.

138. Plaintiff and class members suffered actual injury from having their Personal Information compromised as a result of the Data Breach including, but not limited to: (a) damage to and diminution in the value of their Personal Information, a form of property that Defendants obtained from Plaintiff and class members; (b) violation of their privacy rights; (c) imminent and impending injury arising from the increased risk of identity theft and fraud; and (d) emotional distress.

139. Further, as a result of Defendants' conduct, Plaintiff and class members are forced to live with the anxiety that their Personal Information may be disclosed to the entire world, thereby subjecting them to embarrassment and depriving them of any right to privacy with respect to that information.

140. As a direct and proximate result of Defendant's actions and inactions, Plaintiff and class members have suffered a loss of privacy and are at a present and imminent and increased risk of future harm.

141. Moreover, Plaintiff and class members have an interest in ensuring that their Personal Information, which is believed to remain in the possession of Defendant, 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 Personal Information is not accessible online, is properly encrypted, and that access to such data is password protected.

142. Many failures laid the groundwork for the occurrence of the Data Breach, starting with Defendant's failure to incur the costs necessary to implement adequate and reasonable cyber security training, procedures, and protocols that were necessary to protect Plaintiff's and class members' Personal Information.

143. Defendants maintained the Personal Information in an objectively reckless manner, making the Personal Information vulnerable to unauthorized disclosure.

144. Defendants knew, or reasonably should have known, of the importance of safeguarding Personal Information and of the foreseeable consequences that would result if Plaintiff's and class members' Personal Information was stolen, including the significant costs that would be placed on Plaintiff and class members as a result of the breach.

145. The risk of improper disclosure of Plaintiff's and class members' Personal Information was a known risk to Defendants, and thus Defendants were on notice that failing to take necessary steps to secure Plaintiff's and class members' Personal Information from that risk left the Personal Information in a dangerous condition.

146. Defendants disregarded the rights of Plaintiff and class members by, *inter alia*, (i) intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure that the Personal Information was protected against unauthorized intrusions; (ii) failing to disclose that it did not have robust security protocols and training practices in place to adequately safeguard Plaintiff's and class members' Personal Information; (iii) failing to take standard and reasonably available steps to prevent the Data Breach; (iv) concealing the existence and extent of

the Data Breach for an unreasonable duration of time; and (v) failing to provide Plaintiff and class members prompt and accurate notice of the Data Breach.

CLASS ALLEGATIONS

147. Plaintiff brings this class action individually and on behalf of all members of the following class of similarly situated persons pursuant to Federal Rule of Civil Procedure 23:

Nationwide Class

All persons in the United States whose Personal Information was compromised in the Data Breach publicly disclosed by Defendants on or about February 27, 2024, including all who were sent notice of the Data Breach.

148. Alternatively, or in addition to the nationwide class, Plaintiff seeks to represent the following state class:

Tennessee Class

All persons in Tennessee whose Personal Information was compromised in the Data Breach publicly disclosed by Defendants on or about February 27, 2024, including all who were sent notice of the Data Breach.

149. The nationwide class and the state class are collectively referred to as the "class." Excluded from the class are Defendants and their affiliates, parents, subsidiaries, officers, agents, and directors, as well as the judge(s) presiding over this matter and the clerks of said judge(s).

150. Certification of Plaintiff's claims for class-wide treatment is appropriate because Plaintiff can prove the elements of Plaintiff's claims on a class-wide basis using the same evidence as would be used to prove those elements in individual actions alleging the same claims.

151. Numerosity: The members in the class are so numerous that joinder of all class members in a single proceeding would be impracticable. On information and belief, many hundreds of thousands of individuals' information may have been exposed in the Data Breach.

152. Commonality and Predominance: Common questions of law and fact exist as to all class members and predominate over any potential questions affecting only individual class members. Such common questions of law or fact include, *inter alia*:

a. Whether Defendants had a duty to implement and maintain reasonable security procedures and practices to protect and secure Plaintiff's and class members' Personal Information from unauthorized access and disclosure;

b. Whether Defendants' computer systems and data security practices used to protect Plaintiff's and class members' Personal Information violated the FTC Act and/or state laws and/or Defendants' other duties discussed herein;

c. Whether Defendants failed to adequately respond to the Data Breach, including failing to investigate it diligently and notify affected individuals in the most expedient time possible and without unreasonable delay, and whether this caused damages to Plaintiff and class members;

d. Whether Plaintiff and class members suffered injury as a proximate result of Defendants' negligent actions or failures to act;

e. Whether Defendants failed to exercise reasonable care to secure and safeguard Plaintiff's and class members' Personal Information;

f. Whether an implied contract existed between class members and Defendants providing that Defendants would implement and maintain reasonable security measures to protect and secure class members' Personal Information from unauthorized access and disclosure;

g. Whether injunctive relief is appropriate and, if so, what injunctive relief is necessary to redress the imminent and currently ongoing harm faced by Plaintiff

and class members;

h. Whether Defendants' actions and inactions alleged herein constitute gross negligence;

i. Whether Defendants breached duties to protect Plaintiff's and class members' Personal Information; and

j. Whether Plaintiff and all other members of the class are entitled to damages and the measure of such damages and relief.

153. Defendants engaged in a common course of conduct giving rise to the legal rights sought to be enforced by Plaintiff individually and on behalf of all other class members. Individual questions, if any, pale in comparison, in both quantity and quality, to the numerous common questions that dominate this action.

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

155. Adequacy: Plaintiff will fairly and adequately protect the interests of the class members. Plaintiff is an adequate representative of the class and has no interests adverse to, or conflict with, the class Plaintiff seeks to represent. Plaintiff has retained counsel with substantial experience and success in the prosecution of complex consumer protection class actions of this nature.

156. A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the

management of this class action. The damages and other financial detriment suffered by Plaintiff and all other class members are relatively small compared to the burden and expense that would be required to individually litigate their claims against Defendants, so it would be impracticable for class members to individually seek redress from Defendants' wrongful conduct. Even if class members could afford individual litigation, the court system could not. Individualized litigation creates a potential for inconsistent or contradictory judgments, and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court.

COUNT I
NEGLIGENCE
(On behalf of Plaintiff and the Nationwide Class or, alternatively the Tennessee Class)

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

158. Defendants owed a duty to Plaintiff and all other class members to exercise reasonable care in safeguarding and protecting their PII/PHI in its possession, custody, or control.

159. Defendants knew, or should have known, the risks of collecting and storing Plaintiff's and all other class members' Personal Information and the importance of maintaining secure systems. Defendants knew, or should have known, of the many data breaches that targeted healthcare providers in recent years.

160. Given the nature of Defendants' business, the sensitivity and value of the Personal Information it maintains, and the resources at its disposal, Defendants should have identified the vulnerabilities to its systems and prevented the Data Breach from occurring.

161. Defendants breached these duties by failing to exercise reasonable care in

safeguarding and protecting Plaintiff's and class members' Personal Information by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems to safeguard and protect Personal Information entrusted to it—including Plaintiff's and class members' Personal Information.

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

163. But for Defendants' negligent conduct or breach of the above-described duties owed to Plaintiff and class members, their Personal Information would not have been compromised.

164. As a result of the above-described wrongful actions, inaction, and want of ordinary care that directly and proximately caused the Data Breach, Plaintiff and all other class members have suffered, and will continue to suffer, economic damages and other injury and actual harm in the form of, *inter alia*: (i) a substantially increased risk of identity theft and medical theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (ii) improper disclosure of their PII/PHI; (iii) breach of the confidentiality of their PII/PHI; (iv) deprivation of the value of their PII/PHI, for which there is a well-established national and international market; (v) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of medical identity theft they face and will continue

to face; and (vii) actual or attempted fraud.

COUNT II
NEGLIGENCE PER SE
(On behalf of Plaintiff and the Nationwide Class or, alternatively the Tennessee Class)

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

166. Defendants' duties arise from, *inter alia*, Section 5 of the FTC Act ("FTCA"), 15 U.S.C. § 45(a)(1), which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted by the FTC, the unfair act or practice by a business, such as Defendants, of failing to employ reasonable measures to protect and secure Private Information.

167. Defendants violated Section 5 of the FTCA by failing to use reasonable measures to protect Plaintiff's and all other class members' Personal Information and not complying with applicable industry standards. Defendants' conduct was particularly unreasonable given the nature and amount of Personal Information it obtains and stores, and the foreseeable consequences of a data breach involving Personal Information including, specifically, the substantial damages that would result to Plaintiff and the other class members.

168. Defendants' violations of Section 5 of the FTCA constitutes negligence per se.

169. Plaintiff and class members are within the class of persons that Section 5 of the FTCA were intended to protect.

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

171. It was reasonably foreseeable to Defendants that their failure to exercise reasonable care in safeguarding and protecting Plaintiff's and class members' Personal Information by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data

security processes, controls, policies, procedures, protocols, and software and hardware systems, would result in the release, disclosure, and dissemination of Plaintiff's and class members' Personal Information to unauthorized individuals.

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

COUNT III
BREACH OF FIDUCIARY DUTY
(On behalf of Plaintiff and the Nationwide Class or, alternatively the Tennessee Class)

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

174. Plaintiff and class members either directly or indirectly gave Defendants their Personal Information in confidence, believing that Defendants would protect that information. Plaintiff and class members would not have provided Defendants with this information had they known it would not be adequately protected. Defendants' acceptance and storage of Plaintiff's and class members' Personal Information created a fiduciary relationship between Defendants and

Plaintiff and class members. In light of this relationship, Defendants must act primarily for the benefit of its patients and health plan participants, which includes safeguarding and protecting Plaintiff's and class members' Personal Information.

175. Defendants have a fiduciary duty to act for the benefit of Plaintiff and class members upon matters within the scope of their relationship. It breached that duty by failing to properly protect the integrity of the system containing Plaintiff's and class members' Personal Information, and otherwise failing to safeguard the Personal Information of Plaintiff and class members it collected.

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

COUNT IV
BREACH OF IMPLIED CONTRACT
(On behalf of Plaintiff and the Nationwide Class or, alternatively the Tennessee Class)

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

178. Defendants required Plaintiff and class members to provide, or authorize the

transfer of, their Personal Information in order for Defendants to provide services. In exchange, Defendants entered into implied contracts with Plaintiff and class members in which Defendants agreed to comply with its statutory and common law duties to protect Plaintiff's and class members' Personal Information and to timely notify them in the event of a data breach.

179. Plaintiff and class members would not have provided their Personal Information to Defendant, or would not have agreed to have that information provided to Defendant, had they known that Defendants would not safeguard their Personal Information, as promised, or provide timely notice of a data breach.

180. Plaintiff and class members fully performed their obligations under their implied contracts with Defendant.

181. Defendants breached the implied contracts by failing to safeguard Plaintiff's and class members' Personal Information and by failing to provide them with timely and accurate notice of the Data Breach.

182. The losses and damages Plaintiff and class members sustained (as described above) were the direct and proximate result of Defendant's breach of its implied contracts with Plaintiff and class members.

COUNT V
UNJUST ENRICHMENT
(On behalf of Plaintiff and the Nationwide Class or, alternatively the Tennessee Class)

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

184. This claim is pleaded in the alternative pursuant to Fed. R. Civ. P. 8(d).

185. Plaintiff and class members conferred a monetary benefit upon Defendants in the form of monies paid for healthcare services or other services.

186. Defendants accepted or had knowledge of the benefits conferred upon it by Plaintiff and class members. Defendants also benefitted from the receipt of Plaintiff's and class members' Personal Information.

187. As a result of Defendants' conduct, Plaintiff and class members suffered actual damages in an amount equal to the difference in value between their payments made with reasonable data privacy and security practices and procedures that Plaintiff and class members paid for, and those payments without reasonable data privacy and security practices and procedures that they received.

188. Defendants should not be permitted to retain the money belonging to Plaintiff and class members because Defendants failed to adequately implement the data privacy and security procedures for itself that Plaintiff and class members paid for and that were otherwise mandated by federal, state, and local laws. and industry standards.

189. Defendants should be compelled to provide for the benefit of Plaintiff and class members all unlawful proceeds received by it as a result of its misconduct and the Data Breach.

COUNT VI
BREACH OF CONFIDENCE
(On behalf of Plaintiff and the Nationwide Class or, alternatively the Tennessee Class)

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

191. Plaintiff and class members have an interest, both equitable and legal, in the Personal Information about them that was conveyed or provided to, collected by, and maintained by Defendants, and that was ultimately accessed or compromised in the Data Breach.

192. As a healthcare, pharmaceutical, or health services provider, Defendants have a special relationship to its patients and other affiliated persons, like Plaintiff and the class members.

193. Because of that special relationship, Defendants were provided with and stored private and valuable PHI and other Personal Information related to Plaintiff and the class, which it was required to maintain in confidence.

194. Plaintiff and the class provided Defendants with their Personal Information under both the express and/or implied agreement of Defendants to limit the use and disclosure of such information.

195. Defendants owed a duty to Plaintiff and the class members to exercise the utmost care in obtaining, retaining, securing, safeguarding, deleting, and protecting their Personal Information in its possession from being compromised, lost, stolen, accessed by, misused by, or disclosed to unauthorized persons.

196. Defendants had an obligation to maintain the confidentiality of Plaintiff's and the class members' Personal Information.

197. Plaintiff and the class have a privacy interest in their personal medical matters, and Defendants had a duty not to disclose confidential medical information and records concerning its patients, customers, or other affiliated persons.

198. As a result of the parties' relationship, Defendants had possession and knowledge of confidential Personal Information and confidential medical records of Plaintiff and the class.

199. Plaintiff and the class's Personal Information is not generally known to the public and is confidential by nature.

200. Plaintiff and class members did not consent to nor authorize Defendants to release or disclose their Personal Information to an unknown threat actor.

201. Defendants breached the duties of confidence they owed to Plaintiff and the class when Plaintiff's and class members' Personal Information was disclosed to unknown and

unauthorized parties.

202. Defendants breached its duties of confidence by failing to safeguard Personal Information, including by, among other things: (a) mismanaging its system and failing to identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that resulted in the unauthorized access and compromise of PII and PHI; (b) mishandling its data security by failing to assess the sufficiency of its safeguards in place to control these risks; (c) designing and implementing inadequate cybersecurity safeguards and controls; (d) failing to adequately test and monitor the effectiveness of the safeguards' key controls, systems, and procedures; (e) failing to evaluate and adjust its information security program in light of the circumstances alleged herein; (f) failing to detect the breach at the time it began or within a reasonable time thereafter; (g) failing to follow its on privacy policies and practices published to its patients; (h) storing PHI and medical records/information in an unencrypted and vulnerable manner, allowing its disclosure to hackers; and (i) making an unauthorized and unjustified disclosure and release of Plaintiff and the class members' Personal Information, inclusive of medical records/information to a criminal third party.

203. But for Defendants' wrongful breach of its duty of confidences owed to Plaintiff and the class members, their privacy, confidences, and Personal Information would not have been compromised.

204. As a direct and proximate result of Defendants' breach of confidences, Plaintiff and the class have suffered and/or are at a substantial increased risk of suffering injuries, including:

a. The erosion of the essential and confidential relationship between Defendants and Plaintiff and the class as patients;

b. Loss of the privacy and confidential nature of their PHI;

c. Theft of their PII and/or PHI;

d. Costs associated with the detection and prevention of identity theft or medical identity theft;

e. Costs associated with purchasing credit monitoring and identity theft protection services;

f. Lowered credit scores resulting from credit inquiries following fraudulent activities;

g. Costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Data Breach – including finding fraudulent charges, cancelling and reissuing cards, enrolling in credit monitoring and identity theft protection services, freezing and unfreezing accounts, and imposing withdrawal and purchase limits on compromised accounts;

h. The imminent and certainly impending injury flowing from the increased risk of potential fraud and identity theft posed by their PII and/or PHI being placed in the hands of criminals;

i. Damages to and diminution in value of their PII and PHI entrusted, directly or indirectly, to Defendants with the mutual understanding that Defendants would safeguard Personal Information against theft and not allow access and misuse of their data by others;

j. Continued risk of exposure to hackers and thieves of their PII and/or PHI, which remains in Defendants' possession and is subject to further breaches so long as Defendants fail to undertake appropriate and adequate measures to protect

Plaintiff's and the class members' data;

k. Loss of personal time spent carefully reviewing statements from health insurers and providers to check for charges for services not received, as directed to do by Defendants; and

l. Mental anguish accompanying the loss of confidences and disclosure of their confidential and private PHI.

205. Additionally, Defendants received payments from Plaintiff and the class members for services with the understanding that Defendants would uphold their responsibilities to maintain the confidences of Plaintiff's and class members' private information.

206. Defendants breached the confidence of Plaintiff and the class members when they made an unauthorized release and disclosure of their Personal Information and, accordingly, it would be inequitable for Defendants to retain the benefit at Plaintiff's and class members' expense.

207. As a direct and proximate result of Defendants' breach of their duties, Plaintiff and class members are entitled to damages, including compensatory, punitive, and/or nominal damages, and/or disgorgement or restitution, in an amount to be proven at trial.

PRAYER FOR RELIEF

Plaintiff, individually and on behalf of all other members of the class, respectfully requests that the Court enter judgment in their favor and against Defendants as follows:

A. Certifying the class as requested herein, designating Plaintiff as class representative, and appointing Plaintiff's counsel as Class Counsel;

B. Awarding Plaintiff and the class appropriate monetary relief, including actual damages, statutory damages, punitive damages, restitution, and disgorgement;

C. Awarding Plaintiff and the class equitable, injunctive, and declaratory relief, as may

be appropriate. Plaintiff, individually and on behalf of the class, seeks appropriate injunctive relief designed to prevent Defendants from experiencing another data breach by adopting and implementing best data security practices to safeguard Personal Information and to provide or extend credit monitoring services and similar services to protect against all types of identity theft and medical identity theft;

D. Awarding Plaintiff and the class pre-judgment and post-judgment interest to the maximum extent allowable;

E. Awarding Plaintiff and the class reasonable attorneys' fees, costs, and expenses, as allowable; and

F. Awarding Plaintiff and the class such other favorable relief as allowable under law.

JURY TRIAL DEMANDED

Plaintiff demands a trial by jury of all claims in this Class Action Complaint so triable.

Dated: June 13, 2024

Respectfully submitted,

/s/ Andrew W. Ferich

Andrew W. Ferich (PA ID No. 313696)
AHDOOT & WOLFSON, PC
201 King of Prussia Road, Suite 650
Radnor, PA 19087
Telephone: (310) 474-9111
Facsimile: (310) 474-8585
aferich@ahdootwolfson.com

Raina C. Borelli (*pro hac vice* forthcoming)
STRAUSS BORRELLI PLLC
980 N. Michigan Avenue, Suite 1610
Chicago, IL, 60611
Telephone: (872) 263-1100
Facsimile: (872) 263-1109
raina@straussborrelli.com

Counsel for Plaintiff and the Putative Class

JS 44 (Rev. 04/21)

CIVIL COVER SHEET

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

I. (a) PLAINTIFFS

ROGER WEBB

(b) County of Residence of First Listed Plaintiff Anderson Cty., TN
(EXCEPT IN U.S. PLAINTIFF CASES)

(c) Attorneys *(Firm Name, Address, and Telephone Number)*
Andrew W. Ferich, Ahdoot & Wolfson, PC, 201 King of Prussia Road, Suite 650, Radnor, PA 19087, (310) 474-9111

DEFENDANTS

CENCORA, INC. and THE LASH GROUP, LLC

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

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

Attorneys *(If Known)*

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

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

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

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

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

Click here for: Nature of Suit Code Descriptions.

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

TORTS

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

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

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

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

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

PRISONER PETITIONS

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

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

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

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

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

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

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

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

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

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

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

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

VI. CAUSE OF ACTION

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

Brief description of cause:
Data Breach Class Action

VII. REQUESTED IN COMPLAINT:

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

DEMAND $

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

VIII. RELATED CASE(S) IF ANY

(See instructions): JUDGE Hon, Cynthia M. Rufe DOCKET NUMBER 2:24-cv-02227-CMR

DATE
Jun 13, 2024

SIGNATURE OF ATTORNEY OF RECORD
/s/ Andrew W. Ferich

FOR OFFICE USE ONLY

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

INSTRUCTIONS FOR ATTORNEYS COMPLETING CIVIL COVER SHEET FORM JS 44

Authority For Civil Cover Sheet

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

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

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

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

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

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

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

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

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

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

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

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

UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF PENNSYLVANIA

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

Address of Plaintiff: Anderson County, TN

Address of Defendant: 1 West 1st Avenue, Conshohocken, PA 19428

Place of Accident, Incident or Transaction: Pennsylvania

RELATED CASE IF ANY:
Case Number: 2:24-cv-02227-CMR Judge: Hon. Cynthia M. Rufe Date Terminated n/a

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

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

DATE: 6/13/2024 /s/ Andrew W. Ferich 313696

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
- ☒ X 8. All Other Diversity Cases: *(Please specify)* Data breach class action

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

I, Andrew W. Ferich, counsel of record *or* pro se plaintiff, do hereby certify:

☒ X 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: 6/13/2024 /s/ Andrew W. Ferich 313696

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

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