Multiple Documents

Part	Description
1	1
2	Civil Cover Sheet
3	Designation Form

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

M.W. and F.S., individually and on behalf of all others similarly situated,	)	
Plaintiffs,	)	Case No. 2:24-cv-2672
v.	)	**JURY TRIAL DEMANDED**
CENCORA, INC., Serve at: 1 W 1st Ave. Conshohocken, PA 19428	)	
Defendant.	)	

CLASS ACTION COMPLAINT

COMES NOW Plaintiffs M.W. and F.S., individually and on behalf of all others similarly situated, and on behalf of the general public, upon personal knowledge of facts pertaining to them and upon information and belief as to all other matters, and by and through undersigned counsel, hereby brings this Class Action Complaint against Defendant, Cencora, Inc. (hereinafter, "Cencora" and/or "Defendant"), and alleges as follows:

INTRODUCTION

1. Plaintiffs bring this action on behalf of themselves, and all other individuals similarly situated ("Class Members") against Defendant for its failure to secure and safeguard the protected health information ("PHI") and personally identifiable information ("PII") of thousands of individuals who are customers of the company.

2. Cencora is headquartered in Conshohocken, Pennsylvania and is a company providing drug wholesale services and goods nationwide. In the regular course of its business, Cencora is required to maintain reasonable and adequate security measures to secure, protect, and safeguard their customers' PII against unauthorized access and disclosure.

3. Defendant could have prevented the Data Breach by properly monitoring their file software.

4. Every year, millions of Americans have their most valuable PHI and PII stolen and sold online because of data breaches. Despite the dire warnings about the severe impact of data breaches on Americans of all economic strata, companies still fail to make the necessary investments to implement important and adequate security measures to protect their customers' and employees' data.

5. Defendant required its customers to provide it with their sensitive PHI and PII and failed to protect it. Defendant had an obligation to secure their customers' PHI and PII by implementing reasonable and appropriate data security safeguards. This was part of the bargain between Plaintiffs and Class Members and Defendant.

6. As a result of Defendant's failure to provide reasonable and adequate data security, Plaintiff' and the Class Members' unencrypted, non-redacted PHI and PII has been exposed to unauthorized third parties. Plaintiffs and the Class are now at much higher risk of identity theft and cybercrimes of all kinds, especially considering the highly sensitive PII stolen here and the fact that the compromised PHI and PII is already being sold on the dark web. This risk constitutes a concrete injury suffered by Plaintiffs and the Class as they no longer have control over their PHI and PII, which PHI and PII is now in the hands of third-party cybercriminals. This substantial and imminent risk of identity theft has been recognized by numerous courts as a concrete injury sufficient to establish standing.

7. Plaintiffs and the Class will have to incur costs to pay a third-party credit and identity theft monitoring service for the rest of their lives as a direct result of the Data Breach.

8. Plaintiffs bring this action on behalf of themselves and those similarly situated to seek redress for the lifetime of harm they will now face, including, but not limited to, reimbursement of losses associated with identity theft and fraud, out-of-pocket costs incurred to mitigate the risk of future harm, compensation for time and effort spent responding to the Data Breach, the costs of extending credit monitoring services and identity theft insurance, and injunctive relief requiring Defendant to ensure that they implement and maintain reasonable data security practices going forward.

THE PARTIES

9. Plaintiff M.W. is a resident of Lake Ozark, Camden County, Missouri, whose Personal Information was compromised in the Data Breach.

10. Plaintiff F.S. is a resident of Leawood, Johnson County, Kansas, whose Personal Information was compromised in the Data Breach.

11. Defendant Cencora is a Pennsylvania corporation.

JURISDICTION AND VENUE

12. This Court has subject matter jurisdiction pursuant to the Class Action Fairness Act of 2005 ("CAFA"), 28 U.S.C. §1332(d) because there are more than 100 Class Members, at least one class member is a citizen of a state different from that of Defendant, and the amount in controversy exceeds $5 million, exclusive of interest and costs.

13. Venue is likewise proper in this District pursuant to 28 U.S.C. § 1391(b) because Defendant conducts much of their business in this District and Defendant has caused harm to Class Members residing in this District.

GENERAL ALLEGATIONS COMMON TO ALL COUNTS

14. This is a class action brought by Plaintiffs, individually and on behalf of all citizens who are similarly situated (i.e., the Class Members), seeking to dress Defendant's willful and reckless and violations of their privacy rights. Plaintiffs and the other Class Members were customers of Defendant.

15. For an unspecified period of time, unauthorized third parties accessed and downloaded Plaintiffs' and the Class Members' PHI and PII.

16. This action pertains to Defendant's unauthorized disclosures of the Plaintiffs' PII from February 1, 2024 to May 1, 2024. It is unclear if this Breach originated from Cencora or one of its vendors.

17. Defendant disclosed Plaintiffs' and the other Class Members' PHI and PII to unauthorized persons as a direct and/or proximate result of Defendant's failure to safeguard and protect their PHI and PII.

18. By obtaining, collecting, and storing the PII of Plaintiffs and Class Members, Defendant assumed legal and equitable duties and knew or should have known it was responsible for protecting the PII from unauthorized disclosures.

19. Plaintiffs and Class Members have taken reasonable steps to maintain the confidentiality of their PHI and PII and relied on Defendant to keep their PHI and PII confidential and maintained securely, to use this information for business purposes only, to make only authorized disclosures of this information, and to ensure that any third-party vendors take similar steps.

20. Defendant is a covered entity pursuant to the Health Insurance Portability and Accountability Act ("HIPAA"). *See* 45 C.F.R. § 160.102. Defendant must therefore comply with

the HIPAA Privacy Rule and Security Rule. *See* 45 C.F.R. Part 160 and Part 164, Subparts A through E.

21. Defendant is a covered entity pursuant to the Health Information Technology Act ("HITECH")[1]. *See* 42 U.S.C. §17921, 45 C.F.R. § 160.103.

22. The HIPAA and HITECH rules work in conjunction with the already established laws of privacy Missouri. HIPAA and HITECH do not recognize an individual right of claim for violation but provide the guidelines for the standard of procedure dictating how patient medical information should be kept private.

23. HIPAA's Privacy Rule, otherwise known as "Standards for Privacy of Individually Identifiable Health Information," establishes national standards for the protection of health information.

24. HIPAA's Security Rule, otherwise known as "Security Standards for the Protection of Electronic Protected Health Information," establishes national security standards for the protection of health information that is held or transferred in electronic form. See 42 C.F.R. §§ 164.302-164.318.

25. HIPAA limits the permissible uses of "protected health information" and prohibits the unauthorized disclosure of "protected health information." 45 C.F.R. § 164.502. HIPAA requires that covered entities implement appropriate administrative, technical, and physical safeguards for this information and requires that covered entities reasonably safeguard protected health information from any intentional or unintentional use or disclosure that is in violation of the

[1] HIPAA and HITECH work in tandem to provide guidelines and rules for maintaining protected health information. HITECH references and incorporates HIPAA.

standards, implementation specifications or other requirements of this subpart. *See* 45 C.F.R. § 164.530(c).

26. HIPAA requires a covered entity to have and apply appropriate sanctions against members of its workforce who fail to comply with the privacy policies and procedures of the covered entity or the requirements of 45 C.F.R. Part 164, Subparts D or E. *See* 45 C.F.R. § 164.530(e).

27. HIPAA requires a covered entity to mitigate, to the extent practicable, any harmful effect that is known to the covered entity of a use or disclosure of protected health information in violation of its policies and procedures or the requirements of 45 C.F.R. Part 164, Subpart E by the covered entity or its business associate. *See* 45 C.F.R. § 164.530(f).

28. Under HIPAA:

> Protected health information means individually identifiable health information:
>
> (1) Except as provided in paragraph (2) of this definition, that is:
>
> (i) Transmitted by electronic media;
>
> (ii) Maintained in electronic media; or
>
> (iii) Transmitted or maintained in any other form or medium.[2]

29. HIPAA and HITECH obligated Defendant to implement technical policies and procedures for electronic information systems that maintain electronic protected health information so that such systems were accessible only to those persons or software programs that had been granted access rights and who have a working need to access and view the information. *See* 45 C.F.R. § 164.312(a)(1); *see also* 42 U.S.C. §17902.

[2] 45 C.F.R. § 160.103

30. HIPAA and HITECH also obligated Defendant to implement policies and procedures to prevent, detect, contain, and correct security violations, and to protect against uses or disclosures of electronic protected health information that are reasonably anticipated but not permitted by the privacy rules. *See* 45 C.F.R. § 164.306(a)(1) and § 164.306(a)(3); *see also* 42 U.S.C. §17902.

31. HIPAA further obligated Defendant to ensure that its workforce complied with HIPAA security standard rules (*see* 45 C.F.R. § 164.306(a)(4)) to effectively train its workforces on the policies and procedures with respect to protected health information, as necessary and appropriate for those individuals to carry out their functions and maintain the security of protected health information. *See* 45 C.F.R. § 164.530(b)(1).

32. HIPAA also requires the Office of Civil Rights ("OCR"), within the Department of Health and Human Services ("HHS"), to issue annual guidance documents on the provisions in the HIPAA Security Rule. *See* 45 C.F.R. §§ 164.302-164.318. For example, "HHS has developed guidance and tools to assist HIPAA covered entities in identifying and implementing the most cost effective and appropriate administrative, physical, and technical safeguards to protect the confidentiality, integrity, and availability of e-PHI and comply with the risk analysis requirements of the Security Rule." *See* US Department of Health & Human Services, Security Rule Guidance Material.[3] The list of resources includes a link to guidelines set by the National Institute of Standards and Technology (NIST), which OCR says "represent the industry standard for good

[3] http://www.hhs.gov/hipaa/for-professionals/security/guidance/index.html (last visited June 11, 2024).

business practices with respect to standards for securing e-PHI." *See* US Department of Health & Human Services, Guidance on Risk Analysis.[4]

33. Should a health care provider experience an unauthorized disclosure, it is required to conduct a Four Factor Risk Assessment (HIPAA Omnibus Rule). This standard requires, "A covered entity or business associate must now undertake a four-factor risk assessment to determine whether or not PHI has been compromised and overcome the presumption that the breach must be reported. The four-factor risk assessment focuses on:

> (1) the nature and extent of the PHI involved in the incident (e.g., whether the incident involved sensitive information like social security numbers or infectious disease test results);
>
> (2) the recipient of the PHI;
>
> (3) whether the PHI was actually acquired or viewed; and
>
> (4) the extent to which the risk that the PHI was compromised has been mitigated following unauthorized disclosure (e.g., whether it was immediately sequestered and destroyed)."[5]

34. The HIPAA Breach Notification Rule, 45 CFR §§ 164.400-414, requires HIPAA covered entities and their business associates to provide notification following a breach of unsecured protected health information.

35. The HIPAA Contingency Operations Rule, 45 C.F.R. §164.301(a), requires a healthcare provider to have security measures in place and train its employees and staff so that all its staff and employees know their rolls in facility security.

---

[4] https://www.hhs.gov/hipaa/for-professionals/security/guidance/guidance-risk-analysis/index.html (last visited June 11, 2024).
[5] 78 Fed. Reg. 5641-46, *See also*, 45 C.F.R. §164.304

36. Defendant failed to provide proper notice to Plaintiffs of the disclosure.

37. Defendant failed to conduct or improperly conducted the four factor risk assessment following the unauthorized disclosure.

38. As a direct and/or proximate result of Defendant's wrongful actions and/or inaction and the resulting Breach, the criminal(s) and/or their customers now have Plaintiffs' and the other Class Members' compromised PHI and PII.

39. There is a robust international market for the purloined PHI and PII, specifically medical information. Defendant's wrongful actions and/or inaction and the resulting Breach have also placed Plaintiffs and the other Class Members at an imminent, immediate and continuing increased risk of identity theft, identity fraud[6] and medical fraud.

The Data Breach

40. According to an announcement by Cencora, ("Breach Notice"), "On February 21, 2024, Cencora learned that data from its information systems had been exfiltrated, some of which could contain personal information." Further, "On April 10, 2024, we confirmed that some of your personal information was affected by the incident."

41. On February 21, 2024, Cencora filed a "Material Cybersecurity Incident" Report (also known as an 8k filing) with the U.S. Securities and Exchange Commission identifying the Data Breach incident.[7]

[6] According to the United States Government Accounting Office (GAO), the terms "identity theft" or "identity fraud" are broad terms encompassing various types of criminal activities. Identity theft occurs when PII is used to commit fraud or other crimes. These crimes include, *inter alia,* credit card fraud, phone or utilities fraud, bank fraud and government fraud (theft of government services).

[7] https://d18rn0p25nwr6d.cloudfront.net/CIK-0001140859/81c828c1-699f-45d0-a610-e985f8e8c4b9.pdf (last visited June 11, 2024).

42. Approximately 540,000 victims were notified of the Breach.[8]

43. In its Breach Notice, Cencora identified first names, last names, addresses, dates of birth, health diagnoses, and/or medications and prescriptions as PII potentially obtained in the Data Breach.

44. Absent from the Breach Notice are any details regarding how the Data Breach happened, what Defendant did in response to the Breach, or how Defendant's actions have remediated the root cause of the Data Breach.

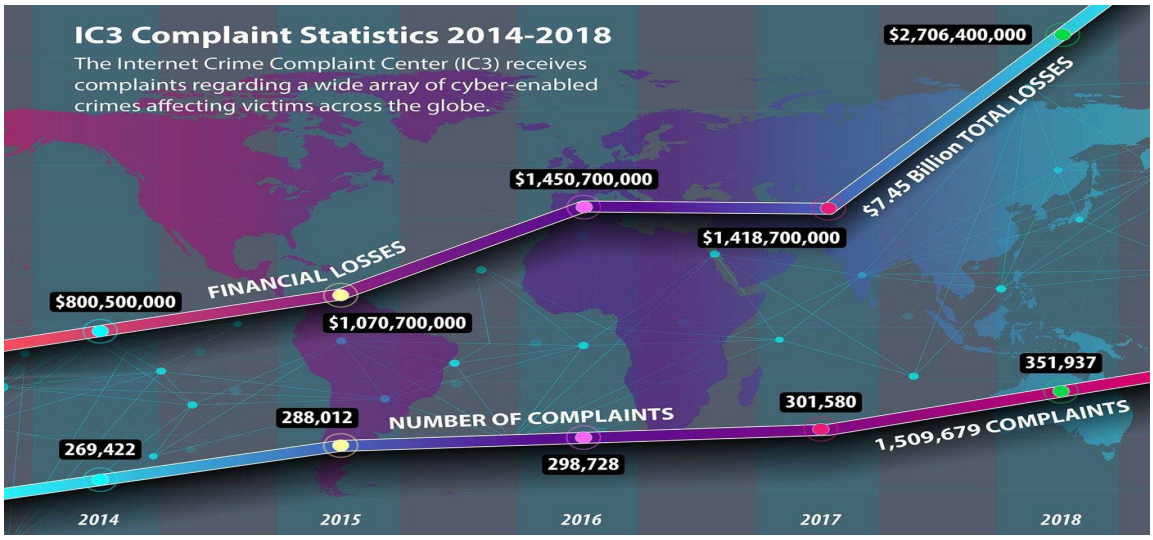
The Data Breach was Preventable

45. Had Defendant Cencora insured that they maintained industry-standard safeguards to monitor, assess, and update security controls and related system risks, Defendant could have ensured sensitive customer data was not transferred to a vendor that was unequipped to protect it. Defendant's lack of oversight of its security controls, and implementation of enhanced security measures only after the Data Breach are inexcusable.

46. Defendant was at all times fully aware of its obligation to protect its customers' PII and the risks associated with failing to do so. Defendant observed frequent public announcements of data breaches affecting finance and insurance industries and knew that information of the type collected, maintained, and stored by Defendant is highly coveted and a frequent target of hackers.

47. This exposure, along with the fact that the compromised PHI and PII is already being sold on the dark web, is tremendously problematic. Cybercrime is rising at an alarming rate, as shown in the FBI's Internet Crime Complaint statistics chart shown below:

[8] https://www.cpomagazine.com/cyber-security/pharmaceutical-giant-cencora-confirms-patient-data-breach-impacting-over-a-dozen-pharma-companies/ (last visited June 11, 2024).



48. By 2013, it was being reported that nearly one out of four data breach notification recipients becomes a victim of identity fraud.[9]

49. Stolen PII is often trafficked on the dark web, as is the case here. Law enforcement has difficulty policing the dark web due to this encryption, which allows users and criminals to conceal identities and online activity.

50. When malicious actors infiltrate companies and copy and exfiltrate the PHI and PII that those companies store, that stolen information often ends up on the dark web because the malicious actors buy and sell that information for profit.[10]

51. In April 2023, NationsBenefits, "disclosed that thousands of its members had their personal information compromised in a late-January ransomware attached targeting Fortra's Anywhere platform, a file-transfer software that the firm was using. According to the news reports,

[9] Pascual, Al, "2013 Identity Fraud Report: Data Breaches Becoming a Treasure Trove for Fraudsters," *Javelin* (Feb. 20, 2013).
[10] *Shining a Light on the Dark Web with Identity Monitoring*, IdentityForce, Dec. 28, 2020, *available at:* https://www.identityforce.com/blog/shining-light-dark-web-identity-monitoring (last visited June 11, 2024).

the ransomeware gang CLOP claimed responsibility for the attack, saying it took advantage of a previously known vulnerability."[11]

52. In mid-April 2023, "the second largest health insurer [Point32Health], in Massachusetts, suffered major technical outages resulting from a ransomware attack. The incident brought down the company's systems that it uses to service members and providers, resulting in some members having difficulty contacting their insurers."[12]

53. In May 2023, MCNA Insurance Company disclosed that "personal health information of nearly nine million patients was compromised in a cyber incident discovered in March. In a data breach notification letter filed with the Maine state attorney general's office dated May 26, the firm said that it detected unauthorized access to its systems on March 6, with some found to be infected with malicious code…According to MCNA, the hackers were successful in accessing patient personal information."[13]

54. In April 2020, ZDNet reported in an article titled, "Ransomeware mentioned in 1,000+ SEC filings over the past year", that "[r]ansomeware gangs are now ferociously aggressive in their pursuit of big companies. They breach networks, use specialized tools to maximize damage, leak corporate information on dark web portals, and even tip journalists to generate negative news complaints as revenge against those who refuse to pay."[14]

55. In September 2020, the United States Cybersecurity and Infrastructure Security Agency published online a "Ransomeware Guide" advising that "[m]alicious actors have adjusted

---

[11] https://www.insurancebusinessmag.com/us/guides/the-insurance-industry-cyber-crime-report-recent-attacks-on-insurance-businesses-448429.aspx (last visited June 11, 2024).
[12] *Id.*
[13] *Id.*
[14] https://www.zdnet.com/article/ransomeware-mentioned-in-1000-sec-filings-over-the-past-year/ (Last visited August 22, 2023).

their ransomware tactics over time to include pressuring victims for payment by threatening to release stolen data if they refuse to pay and publicly naming and shaming victims as secondary forms of extortion."[15]

56. Another example is when the U.S. Department of Justice announced its seizure of AlphaBay in 2017. AlphaBay had more than 350,000 listings, many of which concerned stolen and fraudulent documents that could be used to assume another person's identity. Other marketplaces, similar to the now-defunct AlphaBay, "are awash with [PII] belonging to victims from countries all over the world. One of the key challenges of protecting PII online is its pervasiveness. As data breaches in the news continue to show, PII about employees, customers, and the public is housed in all kinds of organizations, and the increasing digital transformation of today's businesses only broadens the number of potential sources for hackers to target."[16]

57. The PHI and PII of consumers remains of high value to criminals, as evidenced by the price they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[17] Experian reports that a solen credit or

[15] https://www.cisa.gov/sites/default/files/2023-10/StopRansomware-Guide-508C-v3_1.pdf (Last visited June 11, 2024).

[16] *Stolen PII & Ramifications: Identity Theft and Fraud on the Dark Web*, Armor, April 3, 2018, *available at:* https://www.armor.com/resources/blog/stolen-pii-ramifications- identity-theft-fraud-dark-web/.

[17] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends, Oct. 16, 2019, *available at*: https://www.digitaltrends.com/computing/personal- data-sold-on-the-dark-web-how-much-it-costs/.

debit card number can sell for $5 to $110 on the dark web.[18] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[19]

58. Social Security numbers, for example, are among the worst kind of personal information to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change. The Social Security Administration stresses that the loss of an individual's Social Security number, as is the case here, can lead to identity theft and extensive financial fraud:

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number assuming your identity can cause a lot of problems.[20]

59. What is more, it is no easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventative action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraudulent activity to obtain a new number.

60. Even then, a new Social Security number may not be effective. According to July Ferguson of the Identity Theft Resource Center, "The credit bureaus and banks are able to link the

---

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

[19] *In the Dark*, VPNOverview, 2019, *available at*: https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (Last visited June 11, 2024).

[20] Social Security Administration, *Identity Theft and Your Social Security Number*, *available at*: https://www.ssa.gov/pubs/EN-05-10064.pdf (last visited June 11, 2024).

new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[21]

61. Because of this, the information comprised in the Data Breach here is significantly more harmful to lose than the loss of, for example, credit card information in a retailer payment card breach because victims can simply cancel or close credit and debit card accounts. The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change.

62. The PHI and PII compromised in the Data Breach demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information, personally identifiable information and Social Security numbers are worth more than 10 times on the black market."[22]

63. Once PHI and/or PII is sold, it is often used to gain access to various areas of the victim's digital life, including bank accounts, social media, credit card, and tax details. This can lead to additional PHI and PII being harvested from the victim, as well as PII from family, friends, and colleagues of the original victim.

64. According to the FBI's Internet Crime Complaint Center (IC3) 2019 Internet Crime Report, Internet-enabled crimes reached their highest number of complaints and dollar losses in 2019, resulting in more than $3.5 billion in losses to individuals and business victims.

---

[21] Bryan Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), *available at*: http://www.npr.org/2015/02/09/384875839/data-stolen- by-anthem-s-hackers-has-millionsworrying- about-identity-theft.

[22] Time Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, (Feb. 6, 2015), *available at*: https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells- for- 10x-price-of-stolen-credit-card-numbers.html.

65. Victims of identity theft also often suffer embarrassment, blackmail, or harassment in person or online, and/or experience financial losses resulting from fraudulently opened accounts or misuse of existing accounts.

66. Data breaches facilitate identity theft as hackers obtain consumers' PHI and PII and thereafter use it to siphon money from current accounts, open new accounts in the names of their victims, or sell consumers' PHI and PII to others who do the same.

67. For example, the United States Government Accountability Office noted in a June 2007 report on data breaches (the "GAO Report") that criminals use PII to open financial accounts, receive government benefits, and make purchases and secure credit in a victim's name.[23] The GAO Report further notes that this type of identity fraud is the most harmful because it may take some time for a victim to become aware of the fraud, and can adversely impact the victim's credit rating in the meantime. The GAO Report also states that identity theft victims will fact, "substantial costs and inconveniences repairing damage to their credit records… [and their] good name."[24]

68. The exposure of Plaintiffs' and Class Members' PHI and PII to cybercriminals will continue to cause substantial risk of future harm, including identity theft, that is continuing and imminent in light of the many different avenues of fraud and identity theft utilized by third-party cybercriminals to profit off this highly sensitive information.

Defendant Failed to Comply with the Federal Trade Commission

69. Federal and State governments have established security standards and issued recommendations to minimize data breaches and the resulting harm to individuals and financial

[23] *See* Government Accountability Office, *Personal Information: Data Breaches are Frequent, but Evidence of Resulting Identity Theft is Limited; However, the Full Extent is Unknown* (June 2007), https://www.gao.gov/assets/gao-07-737.pdf (last visited June 11, 2024).
[24] *Id.*

institutions. The Federal Trade Commission ("FTC") has issued numerous guides for businesses that highlight the importance of reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[25]

70. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business,* which established guidelines for fundamental data security principals for business.[26] Among other things, the guidelines note businesses should 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 security problems. 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 form the system; and have a response plan ready in the event of a breach.[27]

71. Additionally, the FTC recommends that companies 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.[28]

72. Highlighting the importance of protecting against phishing and other types of data breaches, the FTC has brought enforcement actions against businesses for failing to adequately

---

[25] *See* Federal Trade Commission, *Start With Security* (June 2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last visited June 11, 2024).

[26] *See* Federal Trade Commission, *Protecting Personal Information: A Guide for Business* (Oct. 2016), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited June 11, 2024).

[27] *Id.*

[28] Federal Trade Commission, *Start With Security*, *supra footnote 25*.

and reasonably protect PHI and PII, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

The Impact of Data Breach on Victims

73. Defendant's failure to keep Plaintiffs' and Class Members' PHI and PII secure has severe ramifications. Given the seemingly highly sensitive nature of the PHI and PII stolen in the Data Breach, hackers can commit identity theft, financial fraud, and other identity-related fraud against Plaintiffs and Class Members now and into the indefinite future. As a result, Plaintiffs have suffered injuries and faces an imminent and substantial risk of further injury including identity theft and related cybercrimes due to the Data Breach.

74. The PHI and PII exposed in the Data Breach is highly coveted and valuable on underground markets. Identity thieves can use the PHI and PII to: (a) commit insurance fraud; (b) obtain a fraudulent driver's license or ID card in the victim's name; (c) obtain fraudulent government benefits; (d) file a fraudulent tax return using the victim's information; (e) commit medical and healthcare-related fraud; (f) access financial and investment accounts and records; (g) engage in mortgage fraud; and/or (h) commit any number of other frauds, such as obtaining a job, procuring housing, or giving false information to police during an arrest.

75. Further, malicious actors often wait months or years to use the PHI and PII obtained in data breaches, as victims often become complacent and less diligent in monitoring their accounts after a significant period has passed. These bad actors will also re-use stolen PHI and PII, meaning individuals can be victims of several cybercrimes stemming from a single data breach.

76. Given the confirmed exfiltration of Defendant's customers' PHI and PII from Cencora, many victims of the Data Breach have likely already experienced significant harms as the result of the Data Breach, including, but not limited to, identity theft and fraud. Plaintiffs and Class Members have also spent time, money, and effort dealing with the fallout of the Data Breach, including purchasing credit monitoring services, reviewing financial and insurance statements, checking credit reports, and spending time and effort searching for unauthorized activity.

77. It is no wonder, then, that identity theft exacts a severe emotional toll on its victims. The 2021 Identity Theft Resource Center survey evidences the emotional suffering experienced by victims of identity theft:

- 84% reported anxiety;
- 76% felt violated;
- 32% experienced financial related identity problems;
- 83% reported being turned down for credit or loans;
- 32% reported problems with family members as a result of the breach;
- 10% reported feeling suicidal.[29]

78. Identity theft can also exact a physical toll on its victims. The same survey reported that respondents experienced physical symptoms stemming from their experience with identity theft:

- 48% reported sleep disturbances;
- 37.1% reported an inability to concentrate/lack of focus;
- 28.7% reported they were unable to go to work because of physical symptoms;

[29] https://www.idtheftcenter.org/wp-content/uploads/2021/09/ITRC_2021_Consumer_Aftermath_Report.pdf (Last visited June 11, 2024).

- 23.1 reported new physical illnesses (aches and pains, heart palpitations, sweating, stomach issues); and
- 12.6% reported a start or relapse into unhealthy or addictive behaviors.[30]

79. Annual monetary losses from identity theft are in the billions of dollars. According to a Presidential Report on identity theft produced in 2007:

> In addition to the losses that result when identity thieves fraudulently open accounts…individual victims often suffer indirect financial costs, including the costs incurred in both civil litigation initiated by creditors and in overcoming the many obstacles they face in obtaining or retaining credit. Victims of non-financial identity theft, for example, health-related or criminal record fraud, face other types of harm and frustration.
>
> In addition to out-of-pocket expenses that can reach thousands of dollars for the victims of new account identity theft, and the emotional toll identity theft can take, some victims have to spend what can be a considerable amount of time to repair the damage caused by the identity thieves. Victims of new account identity theft, for example, must correct fraudulent information in their credit reports and monitor their reports for future inaccuracies, close existing bank accounts and open new ones, and dispute charges with individual creditors.

80. The unauthorized disclosure of sensitive PHI and PII to data thieves also reduces its inherent value to its owner, which has been recognized by courts as an independent form of harm.[31]

81. Consumers are injured every time their data is stolen and traded on underground markets, even if they have been victims of previous data breaches. Indeed, the dark web is comprised of multiple discrete repositories of stolen information that can be aggregated together or accessed by different criminal actors who intent to use it for different fraudulent purposes. Each

---

[30] *Id.*

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

data breach increases the likelihood that a victim's personal information will be exposed to more individuals who are seeking to misuse it at the victim's expense.

82. As a result of the wide variety of injuries that can be traced to the Data Breach, Plaintiffs and Class Members have and will continue to suffer economic loss and other actual harm for which they are entitled to damages, including, but not limited to, the following:

a. The unconsented disclosure of confidential information to a third party;

b. Unauthorized use of their PHI and PII without compensation;

c. Losing the value of the explicit and implicit promises of data security;

d. Losing the value of access to their PHI and PII permitted by Defendant without their permission;

e. Identity theft and fraud resulting from the theft of their PHI and PII;

f. Costs associated with the detection and prevention of identity theft and unauthorized use of their financial accounts;

g. Anxiety, emotional distress, and loss of privacy;

h. The present value of ongoing credit monitoring and identity theft protection services necessitated by the Data Breach;

i. Unauthorized charges and loss of use of and access to their accounts;

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

k. Costs associated with time spent and the loss of productivity or the enjoyment of one's life from taking time to address and attempt to mitigate and address the actual and future consequences of the Data Breach, including searching for fraudulent activity, imposing withdrawal and purchase limits on compromised accounts, and the stress, nuisance, and annoyance of dealing with the repercussions of the Data Breach; and

l. The continued, imminent, and certainly impending injury flowing from potential fraud and identity theft posed by their PHI and PII being in the possession of one or more unauthorized third parties.

83. Even in instances where an individual is reimbursed for a financial loss due to identity theft or fraud, that does not make that individual whole again as there is typically significant time and effort associated with seeking reimbursement. The Department of Justice's Bureau of Justice Statistics found that identity theft victims, "reported spending an average of about 7 hours clearing up the issues" relating to identity theft or fraud.[32]

84. Plaintiffs and the Class Members place significant value in data security. According to a survey conducted by cyber-security company FireEye Mandiant, approximately 50% of consumers consider data security to be a main or important consideration when making purchasing decisions and nearly the same percentage would be willing to pay more to work with a provider that has better data security. Seventy percent of consumers would provide less personal information to organizations that suffered a data breach.[33]

85. Plaintiffs and the Class Members have a direct interest in Defendant's promises and duties to protect their PHI and PII, i.e., that Defendant *not increase* their risk of identity theft and fraud. Because Defendant failed to live up to its promises and duties in this respect, Plaintiffs and Class Members seek the present value of ongoing identity protection services to compensate them for the present harm and present and continuing increased risk of harm caused by Defendant's wrongful conduct. Through this remedy, Plaintiffs seek to restore themselves and Class Members as close to the same position as they would have occupied but for Defendant's wrongful conduct, namely its failure to adequately protect Plaintiffs' and the Class Members' PHI and PII.

[32] E. Harrell, U.S. Department of Justice, *Victims of Identity Theft, 2014* (revised Nov. 14, 2017), http://www.bjs.gov/content/pub/pdf/vit14.pdf.

[33] https://web.archive.org/web20220205174527/https://www.fireeye.com/blog/executive-perspective/2016/05/beyond_the_bottomline.html (captured on Feb. 05, 2022).

86. Plaintiffs and the Class Members further seek to recover the value of the unauthorized access to their PHI and PII permitted through Defendant's wrongful conduct. This measure of damages is analogous to the remedies for the unauthorized use of intellectual property. Like a technology covered by a trade secret or patent, use or access to a person's PHI and PII is non-rivalrous—the unauthorized use by. Another does not diminish the rights-holder's ability to practice the patented invention or use the trade-secret protected technology. Nevertheless, a Plaintiff may generally recover the reasonable use of the value of the IP—i.e., a "reasonable royalty" from an infringer. This is true even though the infringer's use did not interfere with the owner's own use (as in the case of a nonpracticing patentee) and even though the owner would not have otherwise licensed such IP to the infringer. A similar royalty or license measure of damages is appropriate here under common law damages principles authorizing recovery of rental or use value. This measure is appropriate because: (a) Plaintiffs and Class Members have a protectible property interest in their PHI and PII; (b) the minimum damages measure for the unauthorized use of personal property is its rental value; (c) rental value is established with reference to market value, i.e., evidence regarding the value of similar transactions.

87. Plaintiffs and the Class Members have an interest in ensuring their PHI and PII is secured and not subject to further theft because Defendant continues to hold their PHI and PII.

CLASS ACTION ALLEGATIONS

88. Pursuant to Rule 23 of the Federal Rules of Civil Procedure, Plaintiffs bring this action on behalf of himself and the following proposed Nationwide class, defined as follows:

Nationwide Class

All persons residing in the United States who are current or former customers of Cencora or any Cencora affiliate, parent, or subsidiary, and had their PHI and/or PII compromised by an unknown third-party cybercriminal as a result of the Data Breach.

In addition, Plaintiff M.W. brings this action on behalf of the following proposed Missouri Subclass, defined as follows:

Missouri Subclass

All persons residing in the State of Missouri who are current or former customers of Cencora or any Cencora affiliate, parent, or subsidiary, and had their PHI and/or PII compromised by an unknown third-party cybercriminal as a result of the Data Breach.

In addition, Plaintiff F.S. brings this action on behalf of the following proposed Kansas Subclass, defined as follows:

Kansas Subclass

All persons residing in the State of Kansas who are current or former customers of Cencora or any Cencora affiliate, parent, or subsidiary, and had their PHI and/or PII compromised by an unknown third-party cybercriminal as a result of the Data Breach.

89. The proposed Nationwide Class, the proposed Missouri Subclass, and the proposed Kansas Subclass will be collectively referred to as the Class, except where it is necessary to differentiate them.

90. Excluded from the proposed Class are any officer or director of Defendant; any officer or director of any affiliate, parent, or subsidiary of Defendant, and/or anyone employed by counsel in this action; and any judge to whom this case is assigned, his or her spouse, and members of the judge's staff.

91. **Numerosity.** Members of the proposed Class likely number in the millions and are thus too numerous to practically join in a single action. Membership in the Class is readily ascertainable from Defendant's own records.

92. **Commonality and Predominance.** Common questions of law and fact exist as to the proposed Class Members and predominate over questions affecting only individual Class Members. These common questions include:

a. Whether Defendant engaged in the wrongful conduct alleged herein;

b. Whether Defendant's inadequate data security measures were a cause of the Data Breach;

c. Whether Defendant owed a legal duty to Plaintiffs and the other Class Members to exercise due care in collecting, storing, and safeguarding their PHI and PII;

d. Whether Defendant negligently or recklessly breached legal duties owed to Plaintiffs and the Class Members to exercise due care in collecting, storing, and safeguarding their PHI and PII;

e. Whether Plaintiffs and the Class are at an increased risk for identity theft because of the Data Breach;

f. Whether Defendant failed to implement and maintain reasonable security procedures and practices for Plaintiffs' and Class Members' PHI and PII in violation of Section 5 of the FTC Act;

g. Whether Plaintiffs and the other Class Members are entitled to equitable relief, including, but not limited to, injunctive relief and restitution.

93. Defendant engaged in a common course of conduct giving rise to the legal rights sought to be enforced by Plaintiffs, individually, and on behalf of the other Class Members. Similar or identical statutory and common violations, business practices, and injuries are involved. Individual questions, if any, pale by comparison, in both quantity and quality, to the numerous questions that dominate this action.

94. **Typicality:** Plaintiffs' claims are typical of the claims of the Members of the Class. All Class Members were subject to the Data Breach and had their PHI and PII accessed by and/or disclosed to unauthorized third parties. Defendant's misconduct affected all Class Members in the same manner.

95. **Adequacy of Representation:** Plaintiffs are adequate representatives of the Class because their interests do not conflict with the interests of the other Class Members they seek to represent; they have retained counsel competent and experienced in complex class action litigation,

and Plaintiffs will prosecute this action vigorously. The interests of the Class will be fairly and adequately protected by Plaintiffs and their counsel.

96. **Superiority:** 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 matter as a class action. The damages, harm, or other financial detriment suffered individually by Plaintiffs and the other Class Members are relatively small compared to the burden and expense that would be required to litigate their claims on an individual basis against Defendant, making it impracticable for Class Members to individually seek redress for Defendant's wrongful conduct. Even if Class Members could afford individual litigation, the court system could not. Individualized litigation would create a potential for inconsistent or contradictory judgments and increase 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, economies of scale, and comprehensive supervision by a single court.

COUNT I
BREACH OF IMPLIED CONTRACT
(On behalf of Plaintiffs and the Nationwide Class and/or the Missouri Subclass and/or the Kansas Subclass)

97. The preceding factual statements and allegations are incorporated herein by reference.

98. Plaintiffs and the other Class Members, as part of their agreement with Defendant, provided Defendant their PHI and PII.

99. Defendant offered services to current or former customers, including Plaintiffs and Class Members, in exchange for monetary payment.

100. As a condition of the purchase, Defendant required Plaintiffs and the Class

Members to provide their PHI and PII. Implied in these exchanges was a promise by Defendant to ensure that the PHI and PII of Plaintiffs and the Class Members in its possession was only used to provide the agreed-upon services from Defendant.

101. These exchanges constituted an agreement between the parties: Plaintiffs and the Class Members would provide their PHI and PII in exchange for the services provided by Defendant.

102. It is clear by these exchanges that the parties intended to enter into an agreement. Plaintiffs and the Class Members would not have disclosed their PHI and PII to Defendant but for the prospect of Defendant's promise of providing the services purchased by Plaintiffs and the Class. Conversely, Defendant presumably would not have taken Plaintiffs' and Class Members' PHI and PII if it did not intend to provide Plaintiffs and Class Members with the bargained-for services.

103. In providing such PHI and PII, Plaintiffs and the other Class Members entered into an implied contract with Defendant, whereby Defendant became obligated to reasonably safeguard Plaintiffs' and the other Class Members' PHI and PII.

104. Under the implied contract, Defendant was obligated to not only safeguard the PHI and PII, but also to provide Plaintiffs and Class Members with prompt, adequate notice of any Data Breach or unauthorized access of said information.

105. Defendant breached the implied contract with Plaintiffs and the other Class Members by failing to take reasonable measures to safeguard their PHI and PII.

106. As a direct result of Defendant's breach of their duty of confidentiality and privacy and the disclosure of Plaintiffs' and the members of the Class confidential personal information, Plaintiffs and the members of the Class suffered damages, including, without limitation, loss of

the benefit of the bargain, exposure to heightened future risk of identity theft, increased infiltrations into their privacy through spam and/or attempted identity theft, loss of privacy, loss of confidentiality, embarrassment, emotional distress, humiliation and loss of enjoyment of life.

107. Plaintiffs and the other Class Members suffered and will continue to suffer damages including, but not limited to: (i) the untimely and/or inadequate notification of the Breach; (ii) improper disclosure of their PHI and PII; (iii) loss of privacy; (iv) out-of-pocket expenses incurred to mitigate the increased risk of identity theft and/or identity fraud pressed upon them by the Breach; (v) the value of their time spent mitigating identity theft and/or identity fraud and/or the increased risk of identity theft and/or identity fraud; (vi) the increased risk of identity theft; and, (vii) emotional distress. At the very least, Plaintiffs and Class Members are entitled to nominal damages.

COUNT II
NEGLIGENCE
(On behalf of Plaintiffs and the Nationwide Class and/or the Missouri Subclass and/or the Kansas Subclass)

108. The preceding factual statements and allegations are incorporated herein by reference.

109. Defendant owed a duty to Plaintiffs and the Class to exercise reasonable care in obtaining, securing, safeguarding, storing, and protecting Plaintiffs' and Class Members' PHI and PII from being compromised, lost, stolen, and accessed by unauthorized persons. This duty includes, among other things, designing, maintaining, and testing its data security systems to ensure that Plaintiffs' and Class Members' PHI and PII in Defendant's possession was adequately secured and protected.

110. Defendant owed, and continues to owe, a duty to Plaintiffs and the other Class Members to safeguard and protect their PHI and PII.

111. Defendant breached their duty by failing to exercise reasonable care and failing to safeguard and protect Plaintiffs' and the other Class Members' PHI and PII.

112. It was reasonably foreseeable that Defendant's failure to exercise reasonable care in safeguarding and protecting Plaintiffs' and the other Class Members' PHI and PII would result in an unauthorized third-party gaining access to such information for no lawful purpose.

113. As a direct result of Defendant's breach of their duty of confidentiality and privacy and the disclosure of Plaintiffs' and the members of the Class confidential personal information, Plaintiffs and the members of the Class suffered damages, including, without limitation, loss of the benefit of the bargain, exposure to heightened future risk of identity theft, increased infiltrations into their privacy through spam and/or attempted identity theft, loss of privacy, loss of confidentiality, embarrassment, emotional distress, humiliation and loss of enjoyment of life.

114. By engaging in the negligent acts and omissions alleged herein, which permitted an unknown third party to access Defendant's systems containing the PHI and PII at issue, Defendant failed to meet the data security standards set forth under Section 5 of the FTC Act, which prohibits "unfair…practices in or affecting commerce." This prohibition includes failing to have adequate data security measures, which Defendant has failed to do as discussed herein.

115. Defendant's failure to meet this standard of data security established under Section 5 of the FTC Act is evidence of negligence.

116. Neither Plaintiffs nor other Class Members contributed to the Data Breach as described in this Complaint.

117. Plaintiffs' and the other Class members suffered and will continue to suffer damages including, but not limited to: (i) the untimely and/or inadequate notification of the Breach; (ii) improper disclosure of their PHI and PII; (iii) loss of privacy; (iv) out-of-pocket expenses

incurred to mitigate the increased risk of identity theft and/or identity fraud pressed upon them by the Breach; (v) the value of their time spent mitigating identity theft and/or identity fraud and/or the increased risk of identity theft and/or identity fraud; (vi) the increased risk of identity theft; and, (vii) emotional distress. At the very least, Plaintiffs and the other Class members are entitled to nominal damages.

118. Defendant's wrongful actions and/or inaction and the resulting Breach (as described above) constituted (and continue to constitute) negligence at common law.

COUNT III
INVASION OF PRIVACY BY PUBLIC DISCLOSURE OF PRIVATE FACTS
(On behalf of Plaintiffs and the Nationwide Class and/or the Missouri Subclass and/or the Kansas Subclass)

119. The preceding factual statements and allegations are incorporated herein by reference.

120. Plaintiffs' and the other Class Members' PHI and PII was (and continues to be) sensitive and personal private information.

121. By virtue of Defendant's failure to safeguard and protect Plaintiffs' and the other Class Members' PHI and PII and the resulting Breach, Defendant wrongfully disseminated Plaintiffs' and the other Class Members' PHI and PII to unauthorized persons.

122. Dissemination of Plaintiffs' and the other Class Members' PHI and PII is not of a legitimate public concern; publicity of their PHI and PII was, is and will continue to be offensive to Plaintiffs, the other Class Members, and all reasonable people. The unlawful disclosure of same violates public mores.

123. As a direct result of Defendant's breach of its duty of confidentiality and privacy and the disclosure of Plaintiffs' and the members of the Class confidential personal information, Plaintiffs and the members of the Class suffered damages, including, without limitation, loss of

the benefit of the bargain, exposure to heightened future risk of identity theft, increased infiltrations into their privacy through spam and/or attempted identity theft, loss of privacy, loss of confidentiality, embarrassment, emotional distress, humiliation and loss of enjoyment of life.

124. Plaintiffs and the other Class members suffered and will continue to suffer damages including, but not limited to: (i) the untimely and/or inadequate notification of the Breach; (ii) improper disclosure of their PHI and PII; (iii) loss of privacy; (iv) out-of-pocket expenses incurred to mitigate the increased risk of identity theft and/or identity fraud pressed upon them by the Breach; (v) the value of their time spent mitigating identity theft and/or identity fraud and/or the increased risk of identity theft and/or identity fraud; (vi) the increased risk of identity theft; and, (vii) emotional distress. At the very least, Plaintiffs and the other Class Members are entitled to nominal damages.

125. Defendant's wrongful actions and/or inaction and the resulting Breach (as described above) constituted (and continue to constitute) an invasion of Plaintiffs' and the other Class Members' privacy by publicly and wrongfully disclosing their private facts (*i.e.*, their PHI and PII) without their authorization or consent.

COUNT IV
BREACH OF FIDUCIARY DUTY OF CONFIDENTIALITY
(On behalf of Plaintiffs and the Nationwide Class and/or the Missouri Subclass and/or the Kansas Subclass)

126. Plaintiffs incorporate the foregoing paragraphs as though fully set forth herein.

127. At all times during Plaintiffs' and Class Members' interactions with Defendant as its customers, Defendant was fully aware of the confidential and sensitive nature of Plaintiffs' and the Class Members' PHI and PII that Plaintiffs and Class Members provided to Defendant.

128. Plaintiffs' and Class Members' PHI and PII constitutes confidential and novel information. Indeed, Plaintiffs' and Class Members' Social Security numbers can be changed only

with great difficulty and time spent, which still enables a threat actor to exploit that information during the interim; additionally, an individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventative action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual ongoing fraudulent activity to obtain a new number.

129. As alleged herein and above, Defendant's relationship with Plaintiffs and Class Members was governed by terms and expectations that Plaintiffs' and Class Members' PHI and PII would be collected, stored, and protected in confidence, and would not be disclosed to unauthorized third parties.

130. Plaintiffs and Class Members provided their respective PHI and PII to Defendant with the explicit and implicit understandings that Defendant would protect and not permit the PHI and PII to be disseminated to any unauthorized parties.

131. Defendant voluntarily received in confidence Plaintiffs' and Class Members' PHI and PII with the understanding that their PHI and PII would not be disclosed or disseminated to the public or any unauthorized third parties.

132. Due to Defendant's failure to prevent, detect, and avoid the Data Breach from occurring by, *inter alia*, not following best information security practices and by not providing proper employee training to secure Plaintiffs' and the Class Members' PHI and PII, Plaintiffs' and Class Members' PHI and PII was disclosed and misappropriated to unauthorized third parties beyond Plaintiffs' and Class Members' confidence, and without their express permission.

133. As a direct and proximate cause of Defendant's actions and/or omissions, Plaintiffs and Class Members have suffered damages.

134. But for Defendant's disclosure of Plaintiffs' and Class Members' PHI and PII, in violation of the parties' understanding of confidentiality, Plaintiffs' and Class Members' PHI and PII would not have been compromised, stolen, viewed, accessed, and used by unauthorized third parties. Defendant's Data Breach was the direct and legal cause of the theft of Plaintiffs' and Class Members' PHI and PII, as well as the resulting damages.

135. The disclosure of Plaintiffs' and Class Members' PHI and PII constituted a violation of Plaintiffs' and Class Members' understanding that Defendant would safeguard and protect the confidential and novel PHI and PII that Plaintiffs and Class Members were required to disclose to Defendant.

136. The concrete injury and harm Plaintiffs and Class Members suffered was the reasonably foreseeable result of Defendant's unauthorized disclosure of Plaintiffs' and Class Members' PHI and PII. Defendant knew their data security procedures for accepting and securing Plaintiffs' and Class Members' PHI and PII had numerous security and other vulnerabilities that placed Plaintiffs' and Class Members' PHI and PII in jeopardy.

137. As a direct and proximate result of Defendant's breaches of confidence, Plaintiffs and Class Members have suffered and/or are at a substantial risk of suffering from damages including, but not limited to: (i) the untimely and/or inadequate notification of the Breach; (ii) improper disclosure of their PHI and PII; (iii) loss of privacy; (iv) out-of-pocket expenses incurred to mitigate the increased risk of identity theft and/or identity fraud pressed upon them by the Breach; (v) the value of their time spent mitigating identity theft and/or identity fraud and/or the increased risk of identity theft and/or identity fraud; (vi) the increased risk of identity theft; and, (vii) emotional distress. At the very least, Plaintiffs and the other Class Members are entitled to nominal damages.

COUNT V
NEGLIGENT TRAINING AND SUPERVISION
(On behalf of Plaintiffs and the Nationwide Class and/or the Missouri Subclass and/or the Kansas Subclass)

138. The preceding factual statements and allegations are incorporated herein by reference.

139. At all times relevant hereto, Defendant owed and currently owe a duty to Plaintiffs and the Class to hire competent employees and agents, and to train and supervise them to ensure they recognize the duties owed to their customers.

140. Defendant breached their duty to Plaintiffs and the members of the Class by allowing its employees and agents to give access to customer PHI and PII to unauthorized users.

141. As a direct result of Defendant's breach of its duty of confidentiality and privacy and the disclosure of Plaintiffs' and the members of the Class confidential personal information, Plaintiffs and the members of the Class suffered damages, including, without limitation, loss of the benefit of the bargain, exposure to heightened future risk of identity theft, increased infiltrations into their privacy through spam and/or attempted identity theft, loss of privacy, loss of confidentiality, embarrassment, emotional distress, humiliation and loss of enjoyment of life.

142. Plaintiffs and the other Class members suffered and will continue to suffer damages including, but not limited to: (i) the untimely and/or inadequate notification of the Breach; (ii) improper disclosure of their PHI and PII; (iii) loss of privacy; (iv) out-of-pocket expenses incurred to mitigate the increased risk of identity theft and/or identity fraud pressed upon them by the Breach; (v) the value of their time spent mitigating identity theft and/or identity fraud and/or the increased risk of identity theft and/or identity fraud; (vi) the increased risk of identity theft; and, (vii) emotional distress. At the very least, Plaintiffs and the other Class Members are entitled to nominal damages.

143. Defendant's wrongful actions and/or inaction and the resulting Breach (as described above) constituted (and continue to constitute) an invasion of Plaintiffs' and the other Class Members' privacy by publicly and wrongfully disclosing their private facts (*i.e.*, their PHI and PII) without their authorization or consent.

COUNT VI
BREACH OF COVENANT OF GOOD FAITH AND FAIR DEALING
(On behalf of Plaintiffs and the Nationwide Class and/or the Missouri Subclass and/or the Kansas Subclass)

144. Plaintiffs incorporate the foregoing paragraphs as though fully set forth herein.

145. As described above, when Plaintiffs and the class Members provided their PHI and PII to Defendant, they entered into implied contracts in which Defendant agreed to comply with its statutory and common law duties and industry standards to protect Plaintiffs' and Class Members' PHI and PII and to timely detect and notify them in the event of a data breach.

146. These exchanges constituted an agreement between the parties: Plaintiffs and Class Members were required to provide their PHI and PII in exchange for services provided by Defendant as well as an implied covenant by Defendant to protect Plaintiffs' and the Class Members' PHI and PII in its possession.

147. It was clear by these exchanges that the parties intended to enter into an agreement. Plaintiffs and Class Members would not have disclosed their PHI and PII to Defendant but for the prospect of Defendant's promise of certain services. Conversely, Defendant presumably would not have taken Plaintiffs' and Class Members' PHI and PII if it did not intend to provide Plaintiffs and Class Members with the services it was offering.

148. Implied in these exchanges was a promise by Defendant to ensure that the PHI and PII of Plaintiffs and Class Members in its possession was only used to provide the agreed-upon services.

149. Plaintiffs and Class Members therefore did not receive the benefit of the bargain with Defendant, because they provided their PHI and PII in exchange for Defendant's implied agreement to keep it safe and secure.

150. While Defendant had discretion in the specifics of how they met the applicable laws and industry standards, this discretion was governed by an implied covenant of good faith and fair dealing.

151. Defendant breached this implied covenant when it engaged in acts and/or omissions that are declared unfair trade practices by the FTC and state statutes and regulations. These acts and omissions included: omitting, suppressing, and concealing the material fact of the inadequacy of the privacy and security protections for Plaintiffs' and Class Members' PHI and PII; storing the PHI and PII of former customers, despite any valid purpose for the storage thereof having ceased upon the termination of the business relationship with those individuals; and failing to disclose to Plaintiffs and Class Members at the time they provided their PHI and PII to it that Defendant's data security systems failed to meet applicable legal and industry standards.

152. Plaintiffs and Class Members did all or substantially all the significant things that the contract required them to do.

153. Likewise, all conditions required for Defendant's performance were met.

154. Defendant's acts and omissions unfairly interfered with Plaintiffs' and Class Members' rights to receive the full benefit of their contracts.

155. Plaintiffs and Class Members have been or will be harmed by Defendant's breach of this implied covenant in the many ways described above, including actual identity theft and/or imminent risk of certainly impending and devastating identity theft that exists now that cyber

criminals have their PHI and PII, and the attendant long-term expense of attempting to mitigate and insure against these risks.

156. Defendant is liable for its breach of these implied covenants, whether or not it is found to have breached any specific, express contractual term.

157. Plaintiffs and Class Members are entitled to damages, including compensatory damages and restitution, declaratory and injunctive relief, and attorneys' fees, costs, and expenses.

COUNT VII
DECLARATORY AND INJUNCTIVE RELIEF
(On behalf of Plaintiffs and the Nationwide Class and/or the Missouri Subclass and/or the Kansas Subclass)

158. Plaintiffs incorporate the foregoing paragraphs as though fully set forth herein.

159. This Count is brought under the federal Declaratory Judgment Act, 28 U.S.C. § 2201.

160. As previously alleged, Plaintiffs and Class Members entered into an implied contract that required Defendant to provide adequate security for the PHI and PII it collected from Plaintiffs and Class Members.

161. Defendant owes a duty of care to Plaintiffs and Class Members requiring it to adequately secure their PHI and PII.

162. Defendant still possesses Plaintiffs' and Class Members' PHI and PII.

163. Since the Data Breach, Defendant has announced few, if any, changes to its data security infrastructure, processes, or procedures to fix the vulnerabilities in its computer systems and/or security practices which permitted the Data Breach to occur and, thereby, prevent future attacks.

164. Defendant has not satisfied its contractual obligations and legal duties to Plaintiffs and Class Members, in fact, now that Defendant's insufficient data security is known to hackers, the PHI and PII in Defendant's possession is even more vulnerable to cyberattack.

165. Actual harm has arisen in the wake of the Data Breach regarding Defendant's contractual obligations and duties of care to provide security measures to Plaintiffs and Class Members. Further, Plaintiffs and Class Members are at risk of additional or further harm due to the exposure of their PHI and PII and Defendant's failure to address the security failings that led to such exposure.

166. There is no reason to believe that Defendant's security measures are any more adequate now than they were before the Data Breach to meet Defendant's contractual obligations and legal duties.

167. Plaintiffs, therefore, seek a declaration (1) that Defendant's existing security measures do not comply with its contractual obligations and duties of care to provide adequate security, and (2) that to comply with its contractual obligations and duties of care, Defendant must implement and maintain reasonable security measures, including, but not limited to:

a. Ordering that Defendant engages third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

b. Ordering that Defendant engages third-party security auditors and internal personnel to run automated security monitoring;

c. Ordering that Defendant audits, tests, and trains its security personnel regarding any new or modified procedures;

d. Ordering that Defendant segments data by, among other things, creating firewalls and access controls so that if one area of Defendant's systems is compromised, hackers cannot gain access to other portions of Defendant's systems;

e. Ordering that Defendant purges, deletes, and destroys in a reasonably secure manner customer data not necessary for its provisions of services;

f. Ordering that Defendant conducts regular computer system scanning and security checks;

g. Ordering that Defendant routinely and continually conducts internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and

h. Ordering Defendant to meaningfully educate its current, former, and prospective customers about the threats they face as a result of the loss of their PHI and PII to third parties, as well as the steps they must take to protect themselves.

REQUEST FOR RELIEF

WHEREFORE, Plaintiffs, individually and on behalf of the other members of the Class proposed in this Petition, respectfully requests that the Court enter judgment in their favor and against Defendant, as follows:

A. Declaring that this action is a proper class action, certifying the Class as requested herein, designating Plaintiffs as Class Representatives and appointing Plaintiffs' counsel as Lead Counsel for the Class;

B. Declaring that Defendant's conduct was extreme and outrageous;

C. Declaring that Defendant breached their implied contract with Plaintiffs and Class Members;

D. Declaring that Defendant negligently disclosed Plaintiffs' and the Class Members PHI and PII;

E. Declaring that Defendant has invaded Plaintiffs' and Class Members' privacy;

F. Declaring that Defendant breached their implied contract with Plaintiffs and the Class Members;

G. Declaring that Defendant was negligent by negligently training and supervising its employees and agents;

H. Ordering Defendant to pay actual damages to Plaintiffs and the Class Members;

I. Ordering Defendant to properly disseminate individualized notice of the Breach to all Class Members;

J. For an Order enjoining Defendant from continuing to engage in the unlawful business practices alleged herein;

K. Ordering Defendant to pay attorneys' fees and litigation costs to Plaintiffs;

L. Ordering Defendant to pay both pre- and post-judgment interest on any amounts awarded; and

M. Ordering such other and further relief as may be just and proper.

JURY DEMAND

Plaintiffs respectfully demand a trial by jury on all of their claims and causes of action so triable.

Dated: June 18, 2024

Respectfully submitted,

/s/ Gary F. Lynch
Gary F. Lynch (PA ID No. 56887)
LYNCH CARPENTER LLP
1133 Penn Avenue, 5th Floor
Pittsburgh, PA 15222
Telephone: (412) 322-9243
gary@lcllp.com

Maureen M. Brady* MO#57800
Lucy McShane* MO#57957
MCSHANE & BRADY, LLC
4006 Central
Kansas City, MO 64111
Telephone: (816) 888-8010
Facsimile: (816) 332-6295
E-mail: mbrady@mcshanebradylaw.com
lmcshane@mcshanebradylaw.com

ATTORNEYS FOR PLAINTIFFS

**pro hac vice forthcoming*

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

M.W. and F.S., individually and on behalf of all others similarly situated,

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

(c) Attorneys *(Firm Name, Address, and Telephone Number)*

Lynch Carpenter LLP, 1133 Penn Avenue, 5th Floor
Pittsburgh, PA 15222, 412-322-9243

DEFENDANTS

CENCORA, INC.

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

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

Attorneys *(If Known)*

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

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

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

(For Diversity Cases Only)

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

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

Click here for: Nature of Suit Code Descriptions.

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

TORTS

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

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

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

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

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

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

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

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

PRISONER PETITIONS

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

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

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

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

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 See attached list DOCKET NUMBER

DATE
Jun 18, 2024

SIGNATURE OF ATTORNEY OF RECORD
/s/ Gary F. Lynch

FOR OFFICE USE ONLY

RECEIPT # AMOUNT APPLYING IFP JUDGE MAG. JUDGE

Additional Related Cases

Case Caption	Case Number	Assigned Judge	Date Terminated
Johnson v. Cencora, Inc. et al	2:24-cv-02227	Cynthia M. Rufe	Case pending
Pettiford v. Cencora, Inc. et al	2:24-cv-02228	Kelley Brisbon Hodge	Case pending
Stoneburner v. Cencora, Inc. et al	2:24-cv-02236	Cynthia M. Rufe	Case pending
Wolford v. Cencora, Inc. et al	2:24-cv-02256	Cynthia M. Rufe	Case pending
Lewis v. Cencora, Inc. et al	2:24-cv-02258	Cynthia M. Rufe	Case pending
McQuillen v. Cencora, Inc. et al	2:24-cv-02271	Gerald J. Pappert	Case pending
Gerber v. Cencora, Inc. et al	2:24-cv-02303	Cynthia M. Rufe	Case pending
James v. Cencora, Inc. et al	2:24-cv-02304	Cynthia M. Rufe	Case pending
Bradford v. Cencora, Inc. et al	2:24-cv-02344	Cynthia M. Rufe	Case pending
Johnson v. Cencora, Inc. et al	2:24-cv-02372	Cynthia M. Rufe	Case pending
Soward v. Cencora, Inc. et al	2:24-cv-02375	Cynthia M. Rufe	Case pending
Turner v. Cencora, Inc. et al	2:24-cv-02416	Cynthia M. Rufe	Case pending
Borne v. Cencora, Inc. et al	2:24-cv-02418	Cynthia M. Rufe	Case pending
Brown v. Cencora, Inc. et al	2:24-cv-02436	Cynthia M. Rufe	Case pending
Strickland v. Cencora, Inc. et al	2:24-cv-02448	Cynthia M. Rufe	Case pending
Lynn v. Cencora, Inc. et al	2:24-cv-02451	Cynthia M. Rufe	Case pending
Moskowitz v. Cencora, Inc. et al	2:24-cv-02453	Cynthia M. Rufe	Case pending
Harrell v. Cencora, Inc. et al	2:24-cv-02524	Cynthia M. Rufe	Case pending
Smith, et al v. Cencora, Inc. et al	2:24-cv-02558	Cynthia M. Rufe	Case pending
Dion v. Cencora, Inc. et al	2:24-cv-02562	Cynthia M. Rufe	Case pending
Russo v. Cencora, Inc.	2:24-cv-02582	Cynthia M. Rufe	Case pending
Castellano v. Cencora, Inc. et al	2:24-cv-02568	Cynthia M. Rufe	Case pending
Webb v. Cencora, Inc. et al	2:24-cv-02603	Cynthia M. Rufe	Case pending
Day, et al v. Cencora, Inc. et al	2:24-cv-02631	Cynthia M. Rufe	Case pending
Buracker v. Cencora, Inc. et al	2:24-cv-02648	Cynthia M. Rufe	Case pending
Reynolds, et al v. Cencora, Inc. et al	2:24-cv-02649	Cynthia M. Rufe	Case pending
Collins-White v. Cencora, Inc. et al	2:24-cv-02662	Unassigned	Case pending

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: Camden County, Missouri; Johnson County, Kansas

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

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

RELATED CASE IF ANY:
Case Number: 2:24-cv-02227 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 ☒
2. Does this case involve the same issue of fact or grow out of the same transaction as a prior suit Pending or within one year previously terminated action in this court? Yes ☒ No ☐
3. Does this case involve the validity or infringement of a patent already in suit or any earlier Numbered case pending or within one year previously terminated action of this court? Yes ☐ No ☒
4. Is this case a second or successive habeas corpus, social security appeal, or pro se case filed by the same individual? Yes ☐ No ☒

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

DATE: June 18, 2024 56887

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

Civil (Place a √ in one category only)

A. Federal Question Cases:

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

B. Diversity Jurisdiction Cases:

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

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

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

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

☒ Relief other than monetary damages is sought.

DATE: June 18, 2024 56887

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.

Additional Related Cases

Case Caption	Case Number	Assigned Judge	Date Terminated
Johnson v. Cencora, Inc. et al	2:24-cv-02227	Cynthia M. Rufe	Case pending
Pettiford v. Cencora, Inc. et al	2:24-cv-02228	Kelley Brisbon Hodge	Case pending
Stoneburner v. Cencora, Inc. et al	2:24-cv-02236	Cynthia M. Rufe	Case pending
Wolford v. Cencora, Inc. et al	2:24-cv-02256	Cynthia M. Rufe	Case pending
Lewis v. Cencora, Inc. et al	2:24-cv-02258	Cynthia M. Rufe	Case pending
McQuillen v. Cencora, Inc. et al	2:24-cv-02271	Gerald J. Pappert	Case pending
Gerber v. Cencora, Inc. et al	2:24-cv-02303	Cynthia M. Rufe	Case pending
James v. Cencora, Inc. et al	2:24-cv-02304	Cynthia M. Rufe	Case pending
Bradford v. Cencora, Inc. et al	2:24-cv-02344	Cynthia M. Rufe	Case pending
Johnson v. Cencora, Inc. et al	2:24-cv-02372	Cynthia M. Rufe	Case pending
Soward v. Cencora, Inc. et al	2:24-cv-02375	Cynthia M. Rufe	Case pending
Turner v. Cencora, Inc. et al	2:24-cv-02416	Cynthia M. Rufe	Case pending
Borne v. Cencora, Inc. et al	2:24-cv-02418	Cynthia M. Rufe	Case pending
Brown v. Cencora, Inc. et al	2:24-cv-02436	Cynthia M. Rufe	Case pending
Strickland v. Cencora, Inc. et al	2:24-cv-02448	Cynthia M. Rufe	Case pending
Lynn v. Cencora, Inc. et al	2:24-cv-02451	Cynthia M. Rufe	Case pending
Moskowitz v. Cencora, Inc. et al	2:24-cv-02453	Cynthia M. Rufe	Case pending
Harrell v. Cencora, Inc. et al	2:24-cv-02524	Cynthia M. Rufe	Case pending
Smith, et al v. Cencora, Inc. et al	2:24-cv-02558	Cynthia M. Rufe	Case pending
Dion v. Cencora, Inc. et al	2:24-cv-02562	Cynthia M. Rufe	Case pending
Russo v. Cencora, Inc.	2:24-cv-02582	Cynthia M. Rufe	Case pending
Castellano v. Cencora, Inc. et al	2:24-cv-02568	Cynthia M. Rufe	Case pending
Webb v. Cencora, Inc. et al	2:24-cv-02603	Cynthia M. Rufe	Case pending
Day, et al v. Cencora, Inc. et al	2:24-cv-02631	Cynthia M. Rufe	Case pending
Buracker v. Cencora, Inc. et al	2:24-cv-02648	Cynthia M. Rufe	Case pending
Reynolds, et al v. Cencora, Inc. et al	2:24-cv-02649	Cynthia M. Rufe	Case pending
Collins-White v. Cencora, Inc. et al	2:24-cv-02662	Unassigned	Case pending

General Information

Case Name	M.W. et al v. CENCORA, INC.
Court	U.S. District Court for the Eastern District of Pennsylvania
Date Filed	Tue Jun 18 00:00:00 EDT 2024
Federal Nature of Suit	Personal Injury: Other [360]
Docket Number	2:24-cv-02672
Parties	F.S.; CENCORA, INC.; M.W.