UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF PENNSYLVANIA

JAMES SOWARD, individually and on behalf of all others similarly situated, Plaintiff, v. CENCORA, INC. AND THE LASH GROUP, LLC, Defendants.	Case No. 24-cv-2375 CLASS ACTION COMPLAINT JURY DEMAND

Plaintiff James Soward ("Plaintiff") brings this class action against Defendants Cencora, Inc. ("Cencora") and the Lash Group, LLC ("Lash Group") (collectively "Defendants" or "Cencora") for its failure to properly secure and safeguard Plaintiff's and Class Members' protected health information ("PHI"), and personally identifiable information ("PII") stored within Defendants' information networks.

INTRODUCTION

1. This class action arises from Defendants' failure to protect highly sensitive data of at least 540,000 Class Members.

2. Defendant Cencora, formerly known as AmerisourceBergen, is a global healthcare and pharmaceutical organization.

3. Defendant Lash Group is a Cencora subsidiary that operates over 100 patient support programs and has served over 15 million patients.

4. Cencora is a multi-billion-dollar company in the global healthcare industry,

primarily involved in pharmaceutical distribution. The company operates across various segments, including pharmaceutical distribution, specialty services, and global commercialization. Cencora's extensive network distributes pharmaceuticals and healthcare products to a wide range of healthcare providers, such as hospitals, clinics, pharmacies, and long-term care facilities. In addition to distribution, Cencora provides support services like consulting, logistics, and reimbursement assistance.

5. Given its broad scope of operations, Defendants' vast handling of data and sensitive information necessitates stringent security measures to protect the privacy of Defendants' clients and patients.

6. Defendants acquired, collected, and stored Plaintiff's and Class Members' PHI/PII.

7. At all relevant times, Defendants knew or should have known that Plaintiff and Class Members would use Defendants' services to store and/or share sensitive data, personal identifiable information ("PII"), and protected health information ("PHI")—together "PHI/PII"—On February 27, 2024, Cencora, Inc. filed a notice with the Securities and Exchange Commission after discovering that an unauthorized party had accessed confidential information on the company's computer network.[1]

8. On no later than February 21, 2024, upon information and belief, unauthorized third-party cybercriminals gained access to Plaintiff's and Class Members' PHI/PII as hosted with Defendants, with the intent of engaging in the misuse of the PHI/PII, including marketing and selling Plaintiff's and Class Members' PHI/PII.

9. The total number of individuals who have had their data exposed due to

[1] *See* https://www.sec.gov/Archives/edgar/data/1140859/000110465924028288/tm247267d1_8k.htm (last accessed May 31, 2024).

Defendants' failure to implement appropriate security safeguards is unknown at this time but is estimated to be in the tens/hundreds of thousands based on Defendants' clientele.

10. "So far, at least 540,000 individuals have been notified in numerous data breach notifications across several states".[2]

11. Personal health information ("PHI") is a category of information that refers to an individual's medical records and history, which is protected under the Health Insurance Portability and Accountability Act ("HIPAA"), which may include test results, procedure descriptions, diagnoses, personal or family medical histories and data points applied to a set of demographic information for a particular patient.

12. Personally identifiable information ("PII") generally incorporates information that can be used to distinguish or trace an individual's identity. It is generally defined to include certain identifiers that do not on their face name an individual, but that are considered to be particularly sensitive and/or valuable if in the wrong hands (for example, Social Security numbers, passport numbers, driver's license numbers, financial account numbers).

13. The vulnerable and potentially exposed data at issue of Plaintiff and the Class stored on Defendants' information network includes, without limitation, name, last name, address, date of birth, health diagnosis, and/or medications and prescriptions.

14. Defendants disregarded the rights of Plaintiff and Class Members by intentionally, willfully, recklessly, or negligently failing to take and implement adequate and reasonable measures to ensure that Plaintiff's and Class Members' PHI/PII was safeguarded, failing to take available steps to prevent unauthorized disclosure of data, and failing to follow applicable, required and appropriate protocols, policies and procedures regarding the encryption

[2] *See* https://www.cpomagazine.com/cyber-security/pharmaceutical-giant-cencora-confirms-patient-data-breach-impacting-over-a-dozen-pharma-companies/ (last accessed May 31, 2024).

of data, even for internal use.

15. As a result, the PHI/PII of Plaintiff and Class Members was compromised through disclosure to an unknown and unauthorized third party—an undoubtedly nefarious third party that seeks to profit off this disclosure by defrauding Plaintiff and Class Members in the future.

16. Plaintiff and Class Members have a continuing interest in ensuring that their information is and remains safe, and they are thus entitled to injunctive and other equitable relief.

JURISDICTION AND VENUE

17. Jurisdiction is proper in this Court under 28 U.S.C. §1332 (diversity jurisdiction). Specifically, this Court has subject matter and diversity jurisdiction over this action under 28 U.S.C. § 1332(d) because this is a class action where the amount in controversy exceeds the sum or value of $5 million, exclusive of interest and costs, there are more than 100 members in the proposed Class, and at least one class member is a citizen of a state different from Defendants.

18. Supplemental jurisdiction to adjudicate issues pertaining to state law is proper in this Court under 28 U.S.C. §1367.

19. Defendants are headquartered and routinely conducts business in the State where this district is located, have sufficient minimum contacts in this State, and have intentionally availed themselves of this jurisdiction by marketing and selling products and services, and by accepting and processing payments for those products and services within this State.

20. Venue is proper in this Court under 28 U.S.C. § 1391 because a substantial part of the events that gave rise to Plaintiff's claims occurred within this District, and Defendants do business in this Judicial District.

THE PARTIES

Plaintiff James Soward

21. Plaintiff James Soward is an adult individual and, at all relevant times herein, a resident and citizen of Arizona residing in Tucson, Arizona. Plaintiff is a victim of the Data Breach.

22. Plaintiff's information was stored with Defendants as a result of their dealings with Defendants.

23. As required in order to obtain services from Defendants, Plaintiff provided Defendants with highly sensitive health and personal information, who then possessed and controlled it.

24. As a result, Plaintiff's information was among the data accessed by an unauthorized third party in the Data Breach.

25. At all times herein relevant, Plaintiff is and was a member of the Class.

26. Plaintiff received a letter from Defendants, dated May 17, 2024, stating that their PHI/PII was involved in the Data Breach (the "Notice").

27. Plaintiff was unaware of the Data Breach until receiving that letter.

28. As a result, Plaintiff was injured in the form of lost time dealing with the consequences of the Data Breach, which included and continues to include: time spent verifying the legitimacy and impact of the Data Breach; time spent exploring credit monitoring and identity theft insurance options; time spent self-monitoring their accounts with heightened scrutiny and time spent seeking legal counsel regarding their options for remedying and/or mitigating the effects of the Data Breach.

29. Plaintiff was also injured by the material risk to future harm they suffer based on

Defendants' breach; this risk is imminent and substantial because Plaintiff's data has been exposed in the breach, the data involved, including Social Security numbers and healthcare information, is highly sensitive and presents a high risk of identity theft or fraud; and it is likely, given Defendants' clientele, that some of the Class's information that has been exposed has already been misused.

30. Plaintiff suffered actual injury in the form of damages to and diminution in the value of their PHI/PII—a condition of intangible property that they entrusted to Defendants, which was compromised in and as a result of the Data Breach.

31. Plaintiff, as a result of the Data Breach, has increased anxiety for their loss of privacy and anxiety over the impact of cybercriminals accessing, using, and selling their PHI/PII.

32. Plaintiff has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from their PHI/PII, in combination with their name, being placed in the hands of unauthorized third parties/criminals.

33. Plaintiff has a continuing interest in ensuring that their PHI/PII, which, upon information and belief, remains backed up in Defendants' possession, is protected and safeguarded from future breaches.

Defendant Cencora, Inc.

34. Defendant Cencora, Inc., is a Pennsylvania corporation headquartered at 1 West First Avenue, Conshohocken, Pennsylvania 19428.

Defendant Lash Group, LLC.

35. Defendant the Lash Group, LLC is a Pennsylvania limited liability corporation headquartered at 1 West First Avenue, Conshohocken, Pennsylvania 19428.

CLASS ACTION ALLEGATIONS

36. Plaintiff brings this action pursuant to the provisions of Rules 23(a), (b)(2), and (b)(3) of the Federal Rules of Civil Procedure, on behalf of themself and the following Class:

> All individuals within the United States of America whose PHI/PII and/or financial information was exposed to unauthorized third parties as a result of the data breach experienced by Defendants on February 21, 2024.

37. Excluded from the Class are the following individuals and/or entities: Defendants and Defendants' parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendants have a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; any and all federal, state or local governments, including but not limited to its departments, agencies, divisions, bureaus, boards, sections, groups, counsels and/or subdivisions; and all judges assigned to hear any aspect of this litigation, as well as its immediate family members.

38. Plaintiff reserves the right to amend the above definitions or to propose subclasses in subsequent pleadings and motions for class certification.

39. This action has been brought and may properly be maintained as a class action under Federal Rule of Civil Procedure Rule 23 because there is a well-defined community of interest in the litigation, and membership in the proposed classes is readily ascertainable.

40. Numerosity: A class action is the only available method for the fair and efficient adjudication of this controversy, as the members of the Class are so numerous that joinder of all members is impractical, if not impossible.

41. Commonality: Plaintiff and the Class Members share a community of interests in that there are numerous common questions and issues of fact and law which predominate

over any questions and issues solely affecting individual members, including, but not necessarily limited to:

a. Whether Defendants had a legal duty to Plaintiff and the Class to exercise due care in collecting, storing, using, and/or safeguarding their PHI/PII;

b. Whether Defendants knew or should have known of the susceptibility of its data security systems to a data breach;

c. Whether Defendants' security procedures and practices to protect its systems were reasonable in light of the measures recommended by data security experts;

d. Whether Defendants' failure to implement adequate data security measures allowed the Data Breach to occur;

e. Whether Defendants failed to comply with their own policies and applicable laws, regulations, and industry standards relating to data security;

f. Whether Defendants adequately, promptly, and accurately informed Plaintiff and Class Members that their PHI/PII had been compromised;

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

h. Whether Defendants' conduct, including their failure to act, resulted in or was the proximate cause of the breach of Defendants' systems, resulting in the loss of the PHI/PII of Plaintiff and Class Members;

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

j. Whether Defendants engaged in unfair, unlawful, or deceptive practices

by failing to safeguard the PHI/PII of Plaintiff and Class Members;

k. Whether Plaintiff and Class Members are entitled to actual and/or statutory damages and/or whether injunctive, corrective and/or declaratory relief and/or accounting is/are appropriate as a result of Defendants' wrongful conduct; and

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

42. Typicality: Plaintiff's claims are typical of the claims of the Class. Plaintiff and all members of the Class sustained damages arising out of and caused by Defendants' common course of conduct in violation of law, as alleged herein.

43. Adequacy of Representation: Plaintiff in this class action is an adequate representative of the Class in that the Plaintiff has the same interest in the litigation of this case as the Class Members, is committed to the vigorous prosecution of this case and has retained competent counsel who are experienced in conducting litigation of this nature.

44. Plaintiff is not subject to any individual defenses unique from those conceivably applicable to other Class Members or the Class in its entirety. Plaintiff anticipates no management difficulties in this litigation.

45. Superiority of Class Action: Since the damages suffered by individual Class Members, while not inconsequential, may be relatively small, the expense and burden of individual litigation by each member make or may make it impractical for members of the Class to seek redress individually for the wrongful conduct alleged herein. Should separate actions be brought or be required to be brought, by each individual member of the Class, the resulting multiplicity of lawsuits would cause undue hardship and expense for the Court and the litigants.

46. The prosecution of separate actions would also create a risk of inconsistent rulings, which might be dispositive of the interests of the Class Members who are not parties to the adjudications and/or may substantially impede their ability to protect their interests adequately.

47. This class action is also appropriate for certification because Defendants have acted or refused to act on grounds generally applicable to Class Members, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members and making final injunctive relief appropriate with respect to the Class in its entirety.

48. Defendants' policies and practices challenged herein apply to and affect Class Members uniformly and Plaintiff's challenge of these policies and practices hinges on Defendants' conduct with respect to the Class in its entirety, not on facts or law applicable only to Plaintiff.

49. Unless a Class-wide injunction is issued, Defendants may continue failing to properly secure the PHI/PII of Class Members, and Defendants may continue to act unlawfully as set forth in this Complaint.

50. Further, Defendants have acted or refused to act on grounds generally applicable to the Class and, accordingly, final injunctive or corresponding declaratory relief with regard to the Class Members as a whole is appropriate under Rule 23(b)(2) of the Federal Rules of Civil Procedure.

COMMON FACTUAL ALLEGATIONS

Defendants Collected/Stored Class Members' PHI/PII

51. Defendants acquired, collected, and stored and assured reasonable security over

Plaintiff's and Class Members' PHI/PII.

52. As a condition of their relationships with Plaintiff and Class Members, Defendants required that Plaintiff and Class Members entrust Defendants with highly sensitive and confidential PHI/PII.

53. Defendants, in turn, stored that information in the part of Defendants' system that was ultimately affected by the Data Breach.

54. By obtaining, collecting, and storing Plaintiff's and Class Members' PHI/PII, Defendants assumed legal and equitable duties and knew or should have known that they were thereafter responsible for protecting Plaintiff's and Class Members' PHI/PII from unauthorized disclosure.

55. Under state and federal law, businesses like Defendants have common law and statutory duties to protect current and former patients' and employees' PII/PHI and to notify them about breaches.

56. Defendants recognize these duties. For example, in its "Privacy Statement Overview," Cencora declares that:

a. Cencora, Inc. and its affiliate companies ("Cencora") value and protect the personal information entrusted to the company by its suppliers, customers, and visitors.[3]

b. Cencora maintains a comprehensive privacy program designed to comply with its legal obligations under applicable law.[4]

[3] *Privacy Statement Overview*, Cencora, (May 31, 2024) https://www.cencora.com/global-privacy-statement-overview

[4] *Id.*

c. We adopt appropriate security measures to protect the Personal Data we process, including sensitive Personal Data. We do not expect that our processing of sensitive Personal Data would impact your rights and interests adversely.[5]

57. Plaintiff and Class Members have taken reasonable steps to maintain the confidentiality of their PHI/PII.

58. Plaintiff and Class Members relied on Defendants to keep their PHI/PII confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

59. Defendants could have prevented the Data Breach, which began no later than February 21, 2024, by adequately securing and encrypting and/or more securely encrypting its servers generally, as well as Plaintiff's and Class Members' PHI/PII.

60. Defendants' negligence in safeguarding Plaintiff's and Class Members' PHI/PII is exacerbated by repeated warnings and alerts directed to protecting and securing sensitive data, as evidenced by the trending data breach attacks in recent years.

61. Yet, despite the prevalence of public announcements of data breach and data security compromises, Defendants failed to take appropriate steps to protect Plaintiff's and Class Members' PHI/PII from being compromised.

Defendants Had an Obligation to Protect the Stolen Information

62. Defendants' failure to adequately secure Plaintiff's and Class Members' sensitive data breaches duties it owes Plaintiff and Class Members under statutory and common law. Under HIPAA, health insurance providers have an affirmative duty to keep patients'

[5] Privacy Statement, Cencora, (May 31, 2024) https://www.cencora.com/global-privacy-statement

Protected Health Information private. As a covered entity, Defendants have a statutory duty under HIPAA and other federal and state statutes to safeguard Plaintiff's and Class Members' data. Moreover, Plaintiff and Class Members surrendered their highly sensitive personal data to Defendants under the implied condition that Defendants would keep it private and secure. Accordingly, Defendants also have an implied duty to safeguard their data, independent of any statute.

63. Because Defendants are covered by HIPAA (45 C.F.R. § 160.102), it is required to comply with the HIPAA Privacy Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and E ("Standards for Privacy of Individually Identifiable Health Information"), and Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C.

64. HIPAA's Privacy Rule or Standards for Privacy of Individually Identifiable Health Information establishes national standards for protecting health information.

65. HIPAA's Privacy Rule or Security Standards for the Protection of Electronic Protected Health Information establishes a national set of security standards for protecting health information that is kept or transferred in electronic form.

66. HIPAA requires Defendants to "comply with the applicable standards, implementation specifications, and requirements" of HIPAA "with respect to electronically protected health information." 45 C.F.R. § 164.302.

67. "Electronic protected health information" is "individually identifiable health information … that is (i) transmitted by electronic media; maintained in electronic media." 45 C.F.R. § 160.103.

68. HIPAA's Security Rule requires Defendants to do the following:

a. Ensure the confidentiality, integrity, and availability of all electronically protected health information the covered entity or business associate creates, receives, maintains, or transmits;

b. Protect against any reasonably anticipated threats or hazards to the security or integrity of such information;

c. Protect against any reasonably anticipated uses or disclosures of such information that are not permitted; and

d. Ensure compliance by its workforce.

69. HIPAA also requires Defendants to "review and modify the security measures implemented … as needed to continue provision of reasonable and appropriate protection of electronically protected health information" under 45 C.F.R. § 164.306(e), and to "[i]mplement technical policies and procedures for electronic information systems that maintain electronically protected health information to allow access only to those persons or software programs that have been granted access rights." 45 C.F.R. § 164.312(a)(1).

70. Moreover, the HIPAA Breach Notification Rule, 45 C.F.R. §§ 164.400-414, requires Defendants to provide notice of the Data Breach to each affected individual "without unreasonable delay and in no case later than 60 days following the discovery of the breach."

71. Defendants were 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."[6]

[6] 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).

72. In addition to its obligations under federal and state laws, Defendants owed a duty to Plaintiff and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the PHI/PII in Defendants' possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons.

73. Defendants owed a duty to Plaintiff and Class Members to provide reasonable security, including consistency with industry standards and requirements, and to ensure that their computer systems, networks, and protocols adequately protected the PHI/PII of Plaintiff and Class Members.

74. Defendants owed a duty to Plaintiff and Class Members to design, maintain, and test their computer systems, servers, and networks to ensure that the PHI/PII was adequately secured and protected.

75. Defendants owed a duty to Plaintiff and Class Members to create and implement reasonable data security practices and procedures to protect the PHI/PII in their possession, including not sharing information with other entities who maintained sub-standard data security systems.

76. Defendants owed a duty to Plaintiff and Class Members to implement processes that would immediately detect a breach in their data security systems in a timely manner.

77. Defendants owed a duty to Plaintiff and Class Members to act upon data security warnings and alerts in a timely fashion.

78. Defendants owed a duty to Plaintiff and Class Members to disclose if their computer systems and data security practices were inadequate to safeguard individuals' PHI/PII and/or financial information from theft because such an inadequacy would be a material fact in the decision to entrust this PHI/PII and/or financial information to Defendants.

79. Defendants owed a duty of care to Plaintiff and Class Members because they were foreseeable and probable victims of any inadequate data security practices.

80. Defendants owed a duty to Plaintiff and Class Members to encrypt and/or more reliably encrypt Plaintiff's and Class Members' PHI/PII and monitor user behavior and activity in order to identify possible threats.

Value of the Relevant Sensitive Information

81. PHI/PII are valuable commodities for which a "cyber black market" exists in which criminals openly post stolen payment card numbers, Social Security numbers, and other personal information on several underground internet websites.

82. 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[7]; Experian reports that a stolen credit or debit card number can sell for $5 to $110 on the dark web[8]; and other sources report that criminals can also purchase access to entire company data breaches from $999 to $4,995.[9]

83. Identity thieves can use PHI/PII, such as that of Plaintiff and Class Members, which Defendants failed to keep secure, to perpetrate a variety of crimes that harm victims—for instance, identity thieves may commit various types of government fraud such as immigration fraud, obtaining a driver's license or identification card in the victim's name but

[7] *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/ (last accessed May 31, 2024).
[8] *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/ (last accessed May 31, 2024).
[9] *In the Dark*, VPNOverview, 2019, *available at*: https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last accessed May 31, 2024).

with another's picture, using the victim's information to obtain government benefits, or filing a fraudulent tax return using the victim's information to obtain a fraudulent refund.

84. There may be a time lag between when harm occurs versus when it is discovered, and also between when PHI/PII and/or financial information is stolen and when it is used: according to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data might be held for up to a year or more before being used to commit identity theft. Further, once stolen data has 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.[10]

85. Here, Defendants knew of the importance of safeguarding PHI/PII and of the foreseeable consequences that would occur if Plaintiff's and Class Members' PHI/PII were stolen, including the significant costs that would be placed on Plaintiff and Class Members as a result of a breach of this magnitude.

86. As detailed above, Defendants are sophisticated organizations with the resources to deploy robust cybersecurity protocols. Defendants knew, or should have known, that the development and use of such protocols were necessary to fulfill their statutory and common law duties to Plaintiff and Class Members. Therefore, their failure to do so is intentional, willful, reckless and/or grossly negligent.

87. 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 its network servers were protected against unauthorized intrusions; (ii)

[10] *Report to Congressional Requesters*, GAO, at 29 (June 2007), *available at:* http://www.gao.gov/new.items/d07737.pdf (last accessed May 31, 2024).

failing to disclose that they did not have adequately robust security protocols and training practices in place to adequately safeguard Plaintiff's and Class Members' PHI/PII; (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.

The Data Breach

88. In February 2024, Cencora disclosed a data breach in a Form 8-K filing with the SEC, stating that unauthorized parties gained access to its information systems and exfiltrated personal data.

89. At the time, Defendants opted not to share any additional information regarding the incident and its potential impact on their clients.

90. Following the detection of the Data Breach on February 21, 2024, Cencora conducted a forensic investigation which confirmed that a threat actor exfiltrated data from Cencora's systems, including patient information provided by its clients for patient support programs.[11]

91. AmerisourceBergen Specialty Group (ABSG), a unit of Cencora, said the breach involved data of a prescription supply program run by the now defunct subsidiary, Medical Initiatives Inc.[12]

92. Explaining the source of the stolen information, the company said it "maintained this information through its partnership with pharmaceutical companies, pharmacies, and healthcare providers in connection with patient support programs, which provide patients access

[11] *More Than a Dozen Pharmaceutical Companies Affected by Cencora Cyberattack*, HIPAA Journal, (May 31, 2024) https://www.hipaajournal.com/cencora-cyberattack-data-breach/
[12] *Id.*

to medications and therapies.[13]

93. Because Cencora has provided almost no information about the Data Breach. It is unknown for precisely how long the cybercriminals had access to Cencora's networks before the breach was discovered. In other words, HealthEC had no effective means to prevent, detect, stop, or mitigate breaches of its systems—thereby allowing cybercriminals unrestricted access to current and former patients' and employees' PHI/PII.

94. On April 10, 2024, Cencora confirmed that the stolen data included first names, last names, addresses, dates of birth, health diagnoses, and/or medications and prescriptions.[14]

95. While the exact number of individuals affected by the Data Breach is currently unknown, Cencora serves more than 18 million patients and handles approximately 20% of the pharmaceuticals distributed in the United States.

96. The total number of impacted individuals is expected to increase. Cencora also warned that all victims may not receive data breach notification letters as it does have all customers' address information to provide direct notifications.

97. Some of the largest drug companies in the world have disclosed data breaches due Cencora'a Data Breach, whom they partner with for pharmaceutical and business service Notifications sent to state Attorneys General so far indicate that the following pharmaceutical companies have been affected: Abbot, AbbVie Inc., Acadia Pharmaceuticals Inc., Bayer Corporation, Bristol Myers Squibb Company and Bristol Myers Squibb Patient Assistance Foundation, Dendreon Pharmaceuticals LLC, Endo Pharmaceuticals Inc., Genentech, Inc., GlaxoSmithKline Group of Companies and the GlaxoSmithKline Patient Access Programs

[13] *Cencora notifies individuals about data stolen earlier this yea*r, Reuters, (May 24, 2024), https://www.reuters.com/technology/cybersecurity/cencora-notifies-individuals-about-cyberattack-earlier-this-year-techcrunch-2024-05-24/

[14] *Id.*

Foundation, Incyte Corporation, Johnson & Johnson Services, Inc. & Johnson & Johnson Patient Assistance Foundation, Inc., Marathon Pharmaceuticals, LLC/PTC Therapeutics, Inc., Novartis Pharmaceuticals Corporation, Pharming Healthcare, Inc., Regeneron Pharmaceuticals, Inc., Sumitomo Pharma America, Inc. / Sunovion Pharmaceuticals Inc., and Tolmar.

Defendants' Failed Response to the Breach

98. Not until after months it claims to have discovered the Data Breach did Defendants begin sending the Notice to persons whose PHI/PII Defendants confirmed was potentially compromised as a result of the Data Breach.

99. The Notice included, *inter alia*, basic details of the Data Breach, Defendants recommended next steps, and Defendants' claims that they had learned of the Data Breach on April 10, 2024, and completed a review thereafter.

100. Upon information and belief, the unauthorized third-party cybercriminals gained access to Plaintiff's and Class Members' PHI/PII with the intent of engaging in the misuse of the PHI/PII, including marketing and selling Plaintiff's and Class Members' PHI/PII.

101. Defendants had and continue to have obligations created by HIPAA, applicable federal and state law as set forth herein, reasonable industry standards, common law, and their own assurances and representations to keep Plaintiff's and Class Members' PHI/PII confidential and to protect such PHI/PII from unauthorized access.

102. Plaintiff and Class Members were required to provide their PHI/PII to Defendants as a result of their dealings, and in furtherance of this relationship, Defendants created, collected, and stored Plaintiff and Class Members with the reasonable expectation and mutual understanding that Defendants would comply with their obligations to keep such information confidential and secure from unauthorized access.

103. Despite this, Plaintiff and the Class Members remain, even today, in the dark regarding what particular data was stolen, the particular malware used, and what steps are being taken, if any, to secure their PHI/PII going forward.

104. Plaintiff and Class Members are, thus, left to speculate as to where their PHI/PII ended up, who has used it, and for what potentially nefarious purposes, and are left to further speculate as to the full impact of the Data Breach and how exactly Defendants intends to enhance their information security systems and monitoring capabilities to prevent further breaches.

105. Unauthorized individuals can now easily access the PHI/PII and/or financial information of Plaintiff and Class Members.

CLAIMS FOR RELIEF

COUNT ONE
Negligence
(On behalf of the Class)

106. Plaintiff realleges and reincorporates every allegation set forth in the preceding paragraphs as though fully set forth herein.

107. At all times herein relevant, Defendants owed Plaintiff and Class Members a duty of care, *inter alia*, to act with reasonable care to secure and safeguard their PHI/PII and to use commercially reasonable methods to do so. Defendants took on this obligation upon accepting and storing the PHI/PII of Plaintiff and Class Members in their computer systems and on their networks.

108. Among these duties, Defendants was expected:

a. to exercise reasonable care in obtaining, retaining, securing,

safeguarding, deleting, and protecting the PHI/PII in their possession;

b. to protect Plaintiff's and Class Members' PHI/PII using reasonable and adequate security procedures and systems that were/are compliant with industry-standard practices;

c. to implement processes to detect the Data Breach quickly and to timely act on warnings about data breaches; and

d. to promptly notify Plaintiff and Class Members of any data breach, security incident, or intrusion that affected or may have affected their PHI/PII.

109. Defendants knew that the PHI/PII was private and confidential and should be protected as private and confidential and, thus, Defendants owed a duty of care not to subject Plaintiff and Class Members to an unreasonable risk of harm because they were foreseeable and probable victims of any inadequate security practices.

110. Defendants knew, or should have known, of the risks inherent in collecting and storing PHI/PII, the vulnerabilities of their data security systems, and the importance of adequate security.

111. Defendants knew about numerous, well-publicized data breaches.

112. Defendants knew, or should have known, that their data systems and networks did not adequately safeguard Plaintiff's and Class Members' PHI/PII.

113. Only Defendants were in the position to ensure that their systems and protocols were sufficient to protect the PHI/PII that Plaintiff and Class Members had entrusted to them.

114. Defendants breached their duties to Plaintiff and Class Members by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard

their PHI/PII.

115. Because Defendants knew that a breach of its systems could damage thousands of individuals, including Plaintiff and Class Members, Defendants had a duty to adequately protect their data systems and the PHI/PII contained therein.

116. Plaintiff's and Class Members' willingness to entrust Defendants with their PHI/PII was predicated on the understanding that Defendants would take adequate security precautions.

117. Moreover, only Defendants had the ability to protect its systems and the PHI/PII is stored on them from attack. Thus, Defendants had a special relationship with Plaintiff and Class Members.

118. Defendants also had independent duties under state and federal laws that required Defendants to reasonably safeguard Plaintiff's and Class Members' PHI/PII and promptly notify them about the Data Breach. These "independent duties" are untethered to any contract between Defendants, Plaintiff, and/or the remaining Class Members.

119. Defendants breached their general duty of care to Plaintiff and Class Members in, but not necessarily limited to, the following ways:

e. by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard the PHI/PII of Plaintiff and Class Members;

f. by failing to timely and accurately disclose that Plaintiff's and Class Members' PHI/PII had been improperly acquired or accessed;

g. by failing to adequately protect and safeguard the PHI/PII by knowingly disregarding standard information security principles, despite obvious

risks, and by allowing unmonitored and unrestricted access to unsecured PHI/PII;

h. by failing to provide adequate supervision and oversight of the PHI/PII with which it was and is entrusted, in spite of the known risk and foreseeable likelihood of breach and misuse, which permitted an unknown third party to gather PHI/PII of Plaintiff and Class Members, misuse the PHI/PII and intentionally disclose it to others without consent.

i. by failing to adequately train its employees not to store PHI/PII longer than absolutely necessary;

j. by failing to consistently enforce security policies aimed at protecting Plaintiff's and the Class Members' PHI/PII;

k. by failing to implement processes to detect data breaches, security incidents, or intrusions quickly; and

l. by failing to encrypt Plaintiff's and Class Members' PHI/PII and monitor user behavior and activity in order to identify possible threats.

120. Defendants' willful failure to abide by these duties was wrongful, reckless, and grossly negligent in light of the foreseeable risks and known threats.

121. As a proximate and foreseeable result of Defendants' grossly negligent conduct, Plaintiff and Class Members have suffered damages and are at imminent risk of additional harm and damages.

122. The law further imposes an affirmative duty on Defendants to timely disclose the unauthorized access and theft of the PHI/PII to Plaintiff and Class Members so that they could and/or still can take appropriate measures to mitigate damages, protect against adverse

consequences and thwart future misuse of their PHI/PII.

123. Defendants breached their duty to notify Plaintiff and Class Members of the unauthorized access by waiting months after learning of the Data Breach to notify Plaintiff and Class Members and then by failing and continuing to fail to provide Plaintiff and Class Members sufficient information regarding the breach.

124. To date, Defendants have not provided sufficient information to Plaintiff and Class Members regarding the extent of the unauthorized access and continue to breach its disclosure obligations to Plaintiff and Class Members.

125. Further, through Defendants' failure to provide timely and clear notification of the Data Breach to Plaintiff and Class Members, Defendants prevented Plaintiff and Class Members from taking meaningful, proactive steps to secure their PHI/PII.

126. There is a close causal connection between Defendants' failure to implement security measures to protect the PHI/PII of Plaintiff and Class Members and the harm suffered, or risk of imminent harm suffered by Plaintiff and Class Members.

127. Plaintiff's and Class Members' PHI/PII was accessed as the proximate result of Defendants (last accessed May 31, 2024). failure to exercise reasonable care in safeguarding such PHI/PII by adopting, implementing, and maintaining appropriate security measures.

128. Defendants wrongful actions, inactions, and omissions constituted (and continue to constitute) common law negligence.

129. The damages Plaintiff and Class Members have suffered (as alleged above) and will suffer were and are the direct and proximate result of Defendants' grossly negligent conduct.

130. As a direct and proximate result of Defendants' negligence and negligence *per*

se, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity of how their PHI/PII is used; (iii) the compromise, publication, and/or theft of their PHI/PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PHI/PII; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to, efforts spent researching how to prevent, detect, contest, and recover from embarrassment and identity theft; (vi) the continued risk to their PHI/PII, which may remain in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' PHI/PII in its continued possession; and (vii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PHI/PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

131. As a direct and proximate result of Defendants' negligence and negligence *per se*, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

132. Additionally, as a direct and proximate result of Defendants' negligence, Plaintiff and Class Members have suffered and will suffer the continued risks of exposure of their PHI/PII, which remain in Defendants' possession and are subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the PHI/PII in its continued possession.

COUNT TWO
Breach of Implied Contract
(On behalf of the Class)

133. Plaintiff realleges and reincorporates every allegation set forth in the preceding paragraphs as though fully set forth herein.

134. Through their course of conduct, Defendants, Plaintiff and Class Members entered into implied contracts for Defendants to implement data security adequate to safeguard and protect the privacy of Plaintiff's and Class Members' PHI/PII.

135. Defendants required Plaintiff and Class Members to provide and entrust their PHI/PII as a condition of obtaining Defendants' services.

136. Defendants solicited and invited Plaintiff and Class Members to provide their PHI/PII as part of Defendants' regular business practices.

137. Plaintiff and Class Members accepted Defendants' offers and provided their PHI/PII to Defendants.

138. As a condition of their relationship with Defendants, Plaintiff and Class Members provided and entrusted their PHI/PII to Defendants.

139. In so doing, Plaintiff and Class Members entered into implied contracts with Defendants by which Defendants agreed to safeguard and protect such non-public information, to keep such information secure and confidential, and to timely and accurately notify Plaintiff and Class Members if their data had been breached and compromised or stolen.

140. A meeting of the minds occurred when Plaintiff and Class Members agreed to, and did, provide their PHI/PII to Defendants, in exchange for, amongst other things, the protection of their PHI/PII.

141. Plaintiff and Class Members fully performed their obligations under the implied contracts

with Defendants.

142. Defendants breached their implied contracts with Plaintiff and Class Members by failing to safeguard and protect their PHI/PII and by failing to provide timely and accurate notice to them that their PHI/PII was compromised as a result of the Data Breach.

143. As a direct and proximate result of Defendants' above-described breach of implied contract, Plaintiff and Class Members have suffered (and will continue to suffer) (a) ongoing, imminent, and impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; (b) actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; (c) loss of the confidentiality of the stolen confidential data; (d) the illegal sale of the compromised data on the dark web; (e) lost work time; and (f) other economic and non-economic harm.

COUNT THREE
Breach of the Implied Covenant of Good Faith and Fair Dealing
(On behalf of the Class)

144. Plaintiff realleges and reincorporates every allegation set forth in the preceding paragraphs as though fully set forth herein.

145. Every contract in this State has an implied covenant of good faith and fair dealing, which is an independent duty and may be breached even when there is no breach of a contract's actual and/or express terms.

146. Plaintiff and Class Members have complied with and performed all conditions of their contracts with Defendants.

147. Defendants breached the implied covenant of good faith and fair dealing by failing to maintain adequate computer systems and data security practices to safeguard PHI/PII, failing to timely and accurately disclose the Data Breach to Plaintiff and Class Members

and continued acceptance of PHI/PII and storage of other personal information after Defendants knew, or should have known, of the security vulnerabilities of the systems that were exploited in the Data Breach.

148. Defendants acted in bad faith and/or with malicious motive in denying Plaintiff and Class Members the full benefit of their bargains as originally intended by the parties, thereby causing them injury in an amount to be determined at trial.

COUNT FOUR
Unjust Enrichment
(On behalf of the Class)

149. Plaintiff realleges and reincorporates every allegation set forth in the preceding paragraphs as though fully set forth herein.

150. By its wrongful acts and omissions described herein, Defendants have obtained a benefit by unduly taking advantage of Plaintiff and Class Members.

151. Defendants, prior to and at the time Plaintiff and Class Members entrusted their PHI/PII to Defendants, caused Plaintiff and Class Members to reasonably believe that Defendants would keep such PHI/PII secure.

152. Defendants were aware, or should have been aware, that reasonable patients and consumers would have wanted their PHI/PII kept secure and would not have contracted with Defendants, directly or indirectly, had they known that Defendants' information systems were sub-standard for that purpose.

153. Defendants were also aware that, if the substandard condition of and vulnerabilities in their information systems were disclosed, it would negatively affect Plaintiff's and Class Members' decisions to seek services therefrom.

154. Defendants failed to disclose facts pertaining to their substandard information systems, defects, and vulnerabilities therein before Plaintiff and Class Members made their

decisions to make purchases, engage in commerce therewith, and seek services or information.

155. Instead, Defendants suppressed and concealed such information. By concealing and suppressing that information, Defendants denied Plaintiff and Class Members the ability to make a rational and informed purchasing and servicing decision and took undue advantage of Plaintiff and Class Members.

156. Defendants were unjustly enriched at the expense of Plaintiff and Class Members, as Defendants received profits, benefits, and compensation, in part, at the expense of Plaintiff and Class Members; however, Plaintiff and Class Members did not receive the benefit of their bargain because they paid for products and or services that did not satisfy the purposes for which they bought/sought them.

157. Since Defendants' profits, benefits, and other compensation were obtained improperly, Defendants are not legally or equitably entitled to retain any of the benefits, compensation, or profits realized from these transactions.

158. Plaintiff and Class Members seek an Order of this Court requiring Defendants to refund, disgorge, and pay as restitution any profits, benefits, and other compensation obtained by Defendants from its wrongful conduct and/or the establishment of a constructive trust from which Plaintiff and Class Members may seek restitution.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of themself and each member of the proposed Class, respectfully request that the Court enter judgment in their favor and for the following specific relief against Defendants as follows:

1. That the Court declare, adjudge, and decree that this action is a proper class

action and certify the proposed Class under F.R.C.P. Rule 23 (b)(1), (b)(2), and/or (b)(3), including the appointment of Plaintiff's counsel as Class Counsel;

2. For an award of damages, including actual, nominal, and consequential damages, as allowed by law in an amount to be determined;

3. That the Court enjoin Defendants, ordering them to cease from unlawful activities;

4. For equitable relief enjoining Defendants from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and Class Members' PHI/PII, and from refusing to issue prompt, complete, and accurate disclosures to Plaintiff and Class Members;

5. For injunctive relief requested by Plaintiff, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and Class Members, including but not limited to an Order:

a. prohibiting Defendants from engaging in the wrongful and unlawful acts described herein;

b. requiring Defendants to protect, including through encryption, all data collected through the course of business in accordance with all applicable regulations, industry standards, and federal, state, or local laws;

c. requiring Defendants to delete and purge the PHI/PII of Plaintiff and Class Members unless Defendants can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and Class Members;

d. requiring Defendants to implement and maintain a comprehensive

Information Security Program designed to protect the confidentiality and integrity of Plaintiff's and Class Members' PHI/PII;

e. requiring Defendants to engage independent third-party security auditors and internal personnel to run automated security monitoring, simulated attacks, penetration tests, and audits on Defendants' systems periodically;

f. prohibiting Defendants from maintaining Plaintiff's and Class Members' PHI/PII on a cloud-based database;

g. requiring Defendants to segment data by creating firewalls and access controls so that, if one area of Defendants' network is compromised, hackers cannot gain access to other portions of Defendants' systems;

h. requiring Defendants to conduct regular database scanning and securing checks;

i. requiring Defendants to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling PHI/PII, as well as protecting the PHI/PII of Plaintiff and Class Members;

j. requiring Defendants to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Defendants' policies, programs, and systems for protecting personal identifying information;

k. requiring Defendants to implement, maintain, review, and revise as necessary a threat management program to monitor Defendants' networks for internal and external threats appropriately, and assess whether monitoring tools are properly configured, tested, and updated; and

l. requiring Defendants to meaningfully educate all Class Members about the threats they face due to the loss of their confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves.

6. For prejudgment interest on all amounts awarded, at the prevailing legal rate;

7. For an award of attorney's fees, costs, and litigation expenses, as allowed by law; and

8. For all other Orders, findings, and determinations identified and sought in this Complaint.

JURY DEMAND

Plaintiff, individually and on behalf of the Class, hereby demands a trial by jury for all issues triable by jury.

Dated: June 2, 2024,

Respectfully submitted,

By: *:/s/ Scott George*

SEEGER WEISS LLP
Scott A. George, Esq. (ID No. 81996)
1515 Market Street, Suite 1380
Philadelphia, PA 19102
Telephone: (215) 564-2300
Email: sgeorge@seegerweiss.com

Christopher A. Seeger*
Christopher L. Ayers*
Jennifer R. Scullion*
Justin M. Smigelsky*
SEEGER WEISS LLP
55 Challenger Road, 6th Floor
Ridgefield Park, New Jersey 07660
Telephone: (973) 639-9100
Facsimile: (973) 639-9393
cseeger@seegerweiss.com
cayers@seegerweiss.com
jscullion@seegerweiss.com
jsmigelsky@seegerweiss.com

LAUKAITIS LAW LLC
Kevin Laukaitis (PA Bar 321670)
954 Avenida Ponce De Leon
Suite 205, #10518
San Juan, PR 00907
T: (215) 789-4462
klaukaitis@laukaitislaw.com

Attorneys for Plaintiff and the Class

**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

JAMES SOWARD, individually and on behalf of all others similarly situated

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

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

Scott A. George, Esq. SeegerWeiss, 1515 Market Street, Suite 1380, Philadelphia, PA 19102, (215) 564-2300,

DEFENDANTS

CENCORA, INC. AND THE LASH GROUP, LLC,

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

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

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

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 $ $5,000,000

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

VIII. RELATED CASE(S) IF ANY

(See instructions): JUDGE Cynthia M. Ruffe DOCKET NUMBER 24-cv-0227

DATE June 2, 2024

SIGNATURE OF ATTORNEY OF RECORD /s/ Scott George

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: 8140 S Vandemoer Ln, Tucson, Arizona 85756

Address of Defendant: 1 West First Ave., Conshohocken, PA 19428 Place of

Accident, Incident or Transaction: Conshohocken, PA

RELATED CASE IF ANY:
Case Number: 2:24-cv-02227 Judge: CYNTHIA M. RUFE Date Terminated

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

1. Is this case related to property included in an earlier numbered suit pending or within one year previously terminated action in this court? Yes ☐ No ☒
2. Does this case involve the same issue of fact or grow out of the same transaction as a prior suit Pending or within one year previously terminated action in this court? Yes ☒ No ☐
3. Does this case involve the validity or infringement of a patent already in suit or any earlier Numbered case pending or within one year previously terminated action of this court? Yes ☐ No ☒
4. Is this case a second or successive habeas corpus, social security appeal, or pro se case filed by the same individual? Yes ☐ No ☒

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

DATE: June 2, 2024 */s/ Scott George* ID No. 81996

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)* *Data breach.*

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

I, Scott A. George, 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: _____ _____ _____

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.