UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF PENNSYLVANIA

BARBARA BURACKER, individually and on behalf of all others similarly situated, Plaintiff, v. CENCORA, INC., THE LASH GROUP, LLC, GLAXOSMITHKLINE, LLC, and GLAXOSMITHKLINE PATIENT ACCESS PROGRAMS FOUNDATION, Defendants.	Case No. 24-cv-2648 **CLASS ACTION** **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Plaintiff Barbara Buracker ("Plaintiff"), individually and on behalf of all others similarly situated (collectively, "Class members"), by and through the undersigned attorneys, brings this Class Action Complaint against Defendants Cencora, Inc. ("Cencora"), The Lash Group, LLC ("Lash Group"), GlaxoSmithKline, LLC, and GlaxoSmithKline Patient Access Programs Foundation (together, "GSK") (collectively, "Defendants"), and complains and alleges upon personal knowledge as to herself and information and belief as to all other matters as follows.

INTRODUCTION

1. Plaintiff brings this class action against Defendants for their failure to secure and safeguard Plaintiff's and Class members' personally identifiable information ("PII") and personal health information ("PHI"), including names, dates of birth, health diagnoses, and medication/prescription information.

2. Cencora is a pharmaceutical solutions and drug wholesale company. Lash Group is a subsidiary of Cencora that provides pharmaceutical sourcing, distribution, and commercialization services. GlaxoSmithKline, LLC is a global biopharmaceutical company, and

GlaxoSmithKline Patient Access Programs Foundation facilitates a program that assists eligible patients in receiving its medications at no cost.

3. On or about February 21, 2024, Cencora and Lash Group discovered that an unauthorized individual or individuals gained access to their network systems obtained the PII/PHI of Plaintiff and Class members (the "Data Breach").

4. Defendants promised Plaintiff and Class members that they would or share Plaintiff and Class members' PII/PHI with third parties who would, implement and maintain reasonable and adequate security measures to secure, protect, and safeguard their PII/PHI against unauthorized access and disclosure. Defendants breached those promises by, *inter alia*, failing to, or sharing PII/PHI with third parties who failed to, implement and maintain reasonable security procedures and practices to protect Plaintiff's and Class members' PII/PHI from unauthorized access and disclosure.

5. As a result of Defendants' inadequate security and breach of their duties and obligations, the Data Breach occurred, and Plaintiff's and Class members' PII/PHI was accessed and disclosed. This action seeks to remedy these failings and their consequences. Plaintiff brings this action on behalf of herself and all persons whose PII/PHI was exposed as a result of the Data Breach.

6. Plaintiff, on behalf of herself and all other Class members, asserts claims for negligence, negligence per se, breach of fiduciary duty, breach of implied contract, unjust enrichment, and violation of the North Carolina Unfair and Deceptive Trade Practices Act, and seeks declaratory relief, injunctive relief, monetary damages, statutory damages, punitive damages, equitable relief, and all other relief authorized by law.

PARTIES

Plaintiff Barbara Buracker

7. Plaintiff Barbara Buracker is a citizen and resident of North Carolina.

8. Plaintiff has been enrolled in a GSK patient assistance program and received related pharmaceutical services from Defendants since approximately 2017. As a condition of receiving services, Defendants required Plaintiff to provide them with her PII/PHI.

9. Based on representations made by Defendants, Plaintiff believed that Defendants had implemented and maintained reasonable security and practices to protect her PII/PHI. With this belief in mind, Plaintiff provided her PII/PHI to Defendants in exchange for receiving patient assistance and pharmaceutical services from Defendant.

10. In connection with providing the patient assistance and pharmaceutical services to Plaintiff, Defendants collected, stored, shared, and maintained Plaintiff's PII/PHI on their systems, including the systems involved in the Data Breach.

11. Had Plaintiff known that Defendants do not adequately protect the PII/PHI in their possession, she would not have agreed to provide Defendants with her PII/PHI or obtained Defendants' patient assistance and pharmaceutical services.

12. Plaintiff received a letter from Cencora notifying her that her PII/PHI was exposed in the Data Breach.

13. As a direct result of the Data Breach, Plaintiff has suffered injury and damages including, *inter alia*, a substantial and imminent risk of identity theft and medical identity theft; the wrongful disclosure and loss of confidentiality of her highly sensitive PII/PHI; deprivation of the value of her PII/PHI; and lost time and money mitigating the effects of the Data Breach; and overpayment for services that did not include adequate data security.

Defendant Cencora, Inc.

14. Defendant Cencora, Inc., is a Delaware corporation with its headquarters located at 1 West First Avenue Conshohocken, Pennsylvania 19428. It may be served through its registered agent: The Corporation Trust Company, 1209 Orange St., Wilmington, Delaware 19801.

Defendant The Lash Group, LLC

15. Defendant The Lash Group, LLC, is a Delaware corporation with its headquarters located at 1 West First Avenue Conshohocken, Pennsylvania 19428. It may be served through its registered agent: CT Corporation System, 600 North Second St., Suite 401, Harrisburg, Pennsylvania 17101.

Defendant GlaxoSmithKline, LLC

16. Defendant GlaxoSmithKline, LLC, is a Delaware corporation with its headquarters located at 2929 Walnut St., Suite 1700, Philadelphia, Pennsylvania 19104. It may be served through its registered agent: CT Corporation System, 600 North Second St., Suite 401, Harrisburg, Pennsylvania 17101.

Defendant GlaxoSmithKline Patient Access Programs Foundation

17. Defendant GlaxoSmithKline Patient Access Programs Foundation is a North Carolina non-profit with its headquarters located at 5 Moore Drive, Research Triangle Park, North Carolina 27709.

JURISDICTION AND VENUE

18. The Court has subject matter jurisdiction over Plaintiff's claims under 28 U.S.C. § 1332(d)(2), because (a) there are 100 or more Class members, (b) at least one Class member is a citizen of a state that is diverse from Defendant's citizenship, and (c) the matter in controversy exceeds $5,000,000, exclusive of interest and costs.

19. This Court has general personal jurisdiction over Defendants Cencora, Lash Group, and GlaxoSmithKline, LLC because they maintain their principal places of business in this District, regularly conduct business in this State, and have sufficient minimum contacts in this State.

20. This Court has general personal jurisdiction over Defendant GlaxoSmithKline Patient Access Programs Foundation because it regularly conducts business in this State, contracts to supply goods or services in this State, and has sufficient minimum contacts in this State.

21. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(b) because Defendants Cencora's, Lash Group's, and GlaxoSmithKline, LLC's principal places of business are in this District and a substantial part of the events, acts, and omissions giving rise to Plaintiff's claims occurred in this District.

FACTUAL ALLEGATIONS

Overview of Defendants

22. Cencora is a "a leading pharmaceutical solutions organization."[1] Cencora "connects manufacturers, providers, pharmacies, and patients" to provide drug distribution and consulting services.[2] Cencora was formerly known as AmerisourceBergen.[3]

[1] *Who we are*, CENCORA, https://www.cencora.com/who-we-are (last accessed June 14, 2024).
[2] *What we offer*, CENCORA, https://www.cencora.com/what-we-offer (last accessed June 14, 2024).
[3] *See AmerisourceBergen becomes Cencora, in alignment with the company's growing global footprint and central role in pharmaceutical access and care*, CENCORA (Aug. 30, 2023), https://www.cencora.com/newsroom/press-releases/amerisourcebergen-becomes-cencora.

23. Lash Group "partners with pharmaceutical companies, pharmacies, and healthcare providers to facilitate access to therapies through drug distribution, patient support and services, business analytics and technology, and other services."[4] Lash Group is a subsidiary of Cencora.[5]

24. GSK is a global biopharma company that develops vaccines, specialty and general medicines.[6] Defendant GlaxoSmithKline Patient Access Programs Foundation is operated by GlaxoSmithKline and provides medications and vaccinations at no or reduced cost to persons meeting certain criteria.[7]

25. In the regular course of its business, including through operating its Patient Access Programs, GSK collects and maintains the PII/PHI of its current and former customers. GSK required Plaintiff and Class members to provide their PII/PHI as a condition of receiving pharmaceutical services.

26. GSK shared Plaintiff and Class members' PII/PHI with Cencora and Lash Group in connection with obtaining services from Cencora and Lash Group.

27. Cencora's website states, "Cencora, Inc. and its affiliate companies ("Cencora") value and protect the personal information entrusted to the company by its suppliers, customers, and visitors. As a United States company doing business around the world, Cencora maintains a

[4] *Notice of Data Security Incident*, LASH GROUP, https://www.lashgroup.com/notice (last accessed June 14, 2024) [hereinafter, the "*Website Notice*"].
[5] *See Our Network*, LASH GROUP, https://www.lashgroup.com/our-network (last accessed June 14, 2024).
[6] *Purpose, strategy, and culture*, GSK, https://us.gsk.com/en-us/company/purpose-strategy-and-culture/ (last accessed June 14, 2024).
[7] GSK Patient Assistance Programs, GSK, https://www.gskforyou.com/content/dam/cf-pharma/gskforyou/master/pdf/GSK-PAP-Information-Sheet.pdf (last accessed June 14, 2024).

comprehensive privacy program designed to comply with its legal obligations under applicable law."[8]

28. Lash Group's website contains a Notice of Privacy Practices (the "Privacy Policy") that "describes how Lash Group may use and disclose your health information."[9] This includes for treatment, payment, and healthcare operations, among others.[10]

29. Lash Group admits it is required by law to follow the Privacy Policy.[11] Lash Group further admits it is required by law to maintain the privacy of protected health information.[12]

30. The Privacy Policy claims "Lash Group respects the confidentiality of your health information and will protect it in a responsible and professional manner."[13]

31. According to the Privacy Policy, Lash Group is required to "obtain your written authorization to use or disclose your health information for reasons other than those listed [in the Privacy Policy] and permitted under law."[14]

32. GSK's website lists its Privacy Principles, which include "Be secure."[15] GSK states, "We respect the privacy of our patients . . . . We inspire trust and are thoughtful when we use personal information."[16] GSK promises to "protect personal information by implementing appropriate safeguards."[17]

---

[8] *Privacy Statement Overview*, CENCORA, https://www.cencora.com/global-privacy-statement-overview (last accessed June 14, 2024).
[9] *Notice of Privacy Practices*, LASH GROUP (July 1, 2012), https://www.lashgroup.com/notice-of-privacy-practices.
[10] *Id.*
[11] *Id.*
[12] *Id.*
[13] *Id.*
[14] *Id.*
[15] *GSK's Privacy Principles*, GSK, https://privacy.gsk.com/en-us/privacy-notice/privacy-principles/ (last accessed June 14, 2024).
[16] *Id.*
[17] *Id.*

33. GSK's website contains a GSK US Privacy Notice (the "GSK Privacy Policy"). The GSK Privacy Policy "sets out how [GSK] collects, uses, transfers, processes, and discloses your data and sets out our security practices."[18] GSK also states, "We respect your privacy and are committed to protecting your personal information."[19]

34. GSK lists the types of PII/PHI it collects in the GSK Privacy Policy, which includes the information affected in the Data Breach.[20]

35. GSK states it will use PII/PHI to, among other things, provide its products and services, "create aggregated and anonymized or de-identified data," for "internal administrative and quality assurance purposes," to "manage and improve our processes and our business operations," and to "[m]anage and protect our network and information systems security."[21]

36. GSK claims it will only "keep your personal information for as long as needed or permitted for the purpose(s) described in this privacy policy and consistent with applicable law."[22]

37. GSK promises it will only "share your personal information on a need-to-know basis, to the extent necessary to follow laws and regulations, and to manage the activities related to our relationship with you."[23] GSK furth claims that, "In some cases, our relationship with you is supported by specialized service providers working on our behalf. These service providers are contractually-required to protect your personal information and not to use it for their own purposes."[24]

---

[18] *Id.*
[19] *Id.*
[20] *See id.*
[21] *Id.*
[22] *Id.*
[23] *Id.*
[24] *Id.*

38. GSK pledges it "will take appropriate legal, organizational, and technical measures to protect your personal information."[25]

39. GSK acknowledges the "need to keep GSK's information and data secure from increasingly sophisticated cyber-attacks and technology misuse."[26] GSK also acknowledges it is responsible for "protecting GSK data that contains information on patients, customers, and employees."[27] Further, "All employees, complementary workers and third-party suppliers who work with personal information (PI) must complete relevant training and ensure they follow our standards."[28]

40. GSK claims it "strives to only conduct business with third parties that commit to maintaining high ethical standards and operate responsibly."[29]

41. Plaintiff and Class members are, or were, patients of GSK, and entrusted GSK with their PII/PHI.

The Data Breach

42. On or about February 21, 2024, Cencora discovered that an unauthorized individual, or unauthorized individuals, accessed and extracted files containing PII/PHI of its' clients' customer.[30] An investigation into the Data Breach determined that personal information was affected in the Data Breach, including patients' names, addresses, dates of birth, health diagnoses, and medication or prescription information.[31]

---

[25] *Id.*
[26] *GSK policies and standards*, GSK, https://www.gsk.com/media/8518/policies-and-standards.pdf (last accessed June 14, 2024).
[27] *Id.*
[28] *Id.*
[29] *Id.*
[30] *See Notice of Data Incident*, CENCORA, https://dojmt.gov/wp-content/uploads/Consumer-notification-letter-1399.pdf (last accessed June 14, 2024) [hereinafter, "*Notice Letter*"].
[31] *Id.*; *Website Notice*, *supra* note 4.

43. According to a data breach notification posted on the Texas Attorney General's website, approximately 66,269 individuals' PII/PHI was compromised during the Data Breach in Texas alone.[32]

44. Cencora and Lash Group did not begin to notify impacted breach victims about the data breach until approximate May 24, 2024, over three months after the Data Breach was discovered.[33] Defendants' failure to promptly notify Plaintiff and Class members that their PII/PHI was accessed and stolen virtually ensured that the unauthorized third parties who exploited those security lapses could monetize, misuse, or disseminate that PII/PHI before Plaintiff and Class members could take affirmative steps to protect their sensitive information. As a result, Plaintiff and Class members will suffer indefinitely from the substantial and concrete risk that their PII/PHI will be misused and their identities will be (or already have been) stolen and misappropriated.

Defendants Knew that Criminals Target PII/PHI

45. At all relevant times, Defendants knew, or should have known, that the PII/PHI they collects, share, and maintain was a target for malicious actors. Indeed, GSK's company policies indicate it was aware of this risk because they notes the "need to keep GSK's information and data secure from increasingly sophisticated cyber-attacks and technology misuse."[34] Despite such knowledge, Defendants failed to implement and maintain reasonable and appropriate data privacy and security measures to protect Plaintiff's and Class members' PII/PHI from cyber-attacks that Defendants should have anticipated and guarded against.

[32] *Data Security Breach Reports*, TEX. ATT'Y GEN., https://oag.my.site.com/datasecuritybreachreport/apex/DataSecurityReportsPage (last accessed June 14, 2024).
[33] *See Notice of Data Incident*, *supra* note 12.
[34] *See GSK policies and standards*, *supra* note 26.

46. It is well known among companies that store sensitive personally identifying information that such information—such as the PII/PHI stolen in the Data Breach—is valuable and frequently targeted by criminals. In a recent article, *Business Insider* noted that "[d]ata breaches are on the rise for all kinds of businesses, including retailers . . . . Many of them were caused by flaws in . . . systems either online or in stores."[35]

47. Cyber criminals seek out PHI at a greater rate than other sources of personal information. In a 2024 report, the healthcare compliance company Protenus found that there were 1,161 medical data breaches in 2023 with over 171 million patient records exposed.[36] This is an increase from the 1,138 medical data breaches which exposed approximately 59 million records that Protenus compiled in 2023.[37]

48. PII/PHI is a valuable property right.[38] The value of PII/PHI as a commodity is measurable.[39] "Firms are now able to attain significant market valuations by employing business models predicated on the successful use of personal data within the existing legal and regulatory frameworks."[40] American companies are estimated to have spent over $19 billion on acquiring

---

[35] Dennis Green, Mary Hanbury & Aine Cain, *If you bought anything from these 19 companies recently, your data may have been stolen*, BUS. INSIDER (Nov. 19, 2019, 8:05 AM), https://www.businessinsider.com/data-breaches-retailers-consumer-companies-2019-1.

[36] *See 2024 Breach Barometer*, PROTENUS 2, https://protenus.com/hubfs/Breach_Barometer/Latest%20Version/Protenus%20-%20Industry%20Report%20-%20Privacy%20-%20Breach%20Barometer%20-%202024.pdf (last accessed June 14, 2024).

[37] *See id*.

[38] *See* Marc van Lieshout, *The Value of Personal Data*, 457 Int'l Fed'n for Info. Processing 26 (May 2015) ("The value of [personal] information is well understood by marketers who try to collect as much data about personal conducts and preferences as possible . . ."), https://www.researchgate.net/publication/283668023_The_Value_of_Personal_Data.

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

[40] Organization for Economic Co-operation and Development, *Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value*, OECD iLIBRARY

personal data of consumers in 2018.[41] It is so valuable to identity thieves that once PII has been disclosed, criminals often trade it on the "cyber black-market," or the "dark web," for many years.

49. As a result of the real and significant value of these data, identity thieves and other cyber criminals have openly posted credit card numbers, SSNs, PII/PHI, and other sensitive information directly on various internet websites making the information publicly available. This information from various breaches, including the information exposed in the Data Breach, can be readily aggregated with other such data and become more valuable to thieves and more damaging to victims.

50. PHI is particularly valuable and has been referred to as a "treasure trove for criminals."[42] A cybercriminal who steals a person's PHI can end up with as many as "seven to ten personal identifying characteristics of an individual."[43]

51. All-inclusive health insurance dossiers containing sensitive health insurance information, names, addresses, telephone numbers, email addresses, SSNs, and bank account information, complete with account and routing numbers, can fetch up to $1,200 to $1,300 each on the black market.[44] According to a report released by the Federal Bureau of Investigation's

(Apr. 2, 2013), https://www.oecd-ilibrary.org/science-and-technology/exploring-the-economics-of-personal-data_5k486qtxldmq-en.

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

[42] *See* Andrew Steager, *What Happens to Stolen Healthcare Data*, HEALTHTECH MAG. (Oct. 20, 2019), https://healthtechmagazine.net/article/2019/10/what-happens-stolen-healthcare-data-perfcon (quoting Tom Kellermann, Chief Cybersecurity Officer, Carbon Black, stating "Health information is a treasure trove for criminals.").

[43] *Id.*

[44] *See* SC Staff, *Health Insurance Credentials Fetch High Prices in the Online Black Market*, SC MAG. (July 16, 2013), https://www.scmagazine.com/news/breach/health-insurance-credentials-fetch-high-prices-in-the-online-black-market.

("FBI") Cyber Division, criminals can sell healthcare records for 50 times the price of a stolen Social Security or credit card number.[45]

52. Criminals can use stolen PII/PHI to extort a financial payment by "leveraging details specific to a disease or terminal illness."[46] Quoting Carbon Black's Chief Cybersecurity Officer, one recent article explained: "Traditional criminals understand the power of coercion and extortion . . . By having healthcare information—specifically, regarding a sexually transmitted disease or terminal illness—that information can be used to extort or coerce someone to do what you want them to do."[47]

53. Consumers place a high value on the privacy of their data, as they should. Researchers shed light on how much consumers value their data privacy—and the amount is considerable. Indeed, studies confirm that "when privacy information is made more salient and accessible, some consumers are willing to pay a premium to purchase from privacy protective websites."[48]

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

---

[45] *See* Federal Bureau of Investigation, *Health Care Systems and Medical Devices at Risk for Increased Cyber Intrusions for Financial Gain* (April 8, 2014), https://www.illuminweb.com/wp-content/uploads/ill-mo-uploads/103/2418/health-systems-cyber-intrusions.pdf.
[46] Steager, *supra* note 42.
[47] *Id.*
[48] Janice Y. Tsai et al., *The Effect of Online Privacy Information on Purchasing Behavior*, *An Experimental Study*, 22(2) INFO. SYS. RSCH. 254 (June 2011) https://www.jstor.org/stable/23015560?seq=1.

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

55. Theft of PII/PHI can have serious consequences for the victim. The FTC warns consumers that identity thieves use PII/PHI to receive medical treatment, start new utility accounts, and incur charges and credit in a person's name.[49] [50]

56. Experian, one of the largest credit reporting companies in the world, warns consumers that "[i]dentity thieves can profit off your personal information" by, among other things, selling the information, taking over accounts, using accounts without permission, applying for new accounts, obtaining medical procedures, filing a tax return, and applying for government benefits.[51]

57. Identity theft is not an easy problem to solve. In a survey, the Identity Theft Resource Center found that almost 20% of victims of identity misuse needed more than a month to resolve issues stemming from identity theft.[52]

58. Theft of PII is even more serious when it includes theft of PHI. Data breaches involving medical information "typically leave[] a trail of falsified information in medical records

[49] *See* Federal Trade Commission, *What to Know About Identity Theft*, FTC CONSUMER INFO., https://www.consumer.ftc.gov/articles/what-know-about-identity-theft (last accessed June 14, 2024).

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

[51] *See* Louis DeNicola, *What Can Identity Thieves Do with Your Personal Information and How Can You Protect Yourself*, EXPERIAN (May 21, 2023), https://www.experian.com/blogs/ask-experian/what-can-identity-thieves-do-with-your-personal-information-and-how-can-you-protect-yourself/.

[52] Identity Theft Resource Center, *2023 Consumer Aftermath Report*, IDENTITY THEFT RES. CTR. (2023), https://www.idtheftcenter.org/publication/2023-consumer-impact-report/ (last accessed June 14, 2024).

that can plague victims' medical and financial lives for years."[53] It "is also more difficult to detect, taking almost twice as long as normal identity theft."[54] In warning consumers on the dangers of medical identity theft, the FTC states that an identity thief may use PII/PHI "to see a doctor, get prescription drugs, buy medical devices, submit claims with your insurance provider, or get other medical care." [55] The FTC also warns, "If the thief's health information is mixed with yours it could affect the medical care you're able to get or the health insurance benefits you're able to use."[56]

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

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

b. Significant bills for medical goods and services neither sought nor received.

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

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

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

---

[53] Pam Dixon & John Emerson, *The Geography of Medical Identity Theft*, WORLD PRIV. F. (Dec. 12, 2017), http://www.worldprivacyforum.org/wp-content/uploads/2017/12/WPF_Geography_of_Medical_Identity_Theft_fs.pdf.
[54] *See* Federal Bureau of Investigation, *Health Care Systems and Medical Devices at Risk . . .*, *supra* note 45.
[55] *See* Federal Trade Commission, *What to Know About Medical Identity Theft*, FTC CONSUMER INFO., https://www.consumer.ftc.gov/articles/what-know-about-medical-identity-theft (last accessed June 14, 2024).
[56] *Id*.

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

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

h. Sales of medical debt arising from identity theft can perpetuate a victim's debt collection and credit problems, through no fault of their own. [57]

60. There may also be time lags between when sensitive personal information is stolen, when it is used, and when a person discovers it has been used. On average it takes approximately three months for consumers to discover their identity has been stolen and used, but it takes some individuals up to three years to learn that information.[58]

61. It is within this context that Plaintiff and all other Class members must now live with the knowledge that their PII/PHI is forever in cyberspace and was taken by people intending to use that information for any number of improper purposes and scams, including making the information available for sale on the black-market.

Damages Sustained by Plaintiff and the Other Class Members

62. Plaintiff and all other Class members have suffered injury and damages, including, but not limited to: (i) a substantially increased and imminent risk of identity theft and medical identity theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (ii) improper disclosure of their PII/PHI; (iii) breach of the confidentiality of their PII/PHI; (iv) deprivation of the value of their PII/PHI, for which there is a well-established national and international market; (v) lost time and money incurred to mitigate

[57] *See* Dixon & Emerson, *supra* note 53.
[58] John W. Coffey, *Difficulties in Determining Data Breach Impacts*, 17 J. OF SYSTEMICS, CYBERNETICS AND INFORMATICS 9 (2019), http://www.iiisci.org/journal/pdv/sci/pdfs/IP069LL19.pdf.

and remediate the effects of the Data Breach, including the increased risks of identity theft and medical identity theft they face and will continue to face; and (vi) overpayment for the services that were received without adequate data security.

CLASS ALLEGATIONS

63. This action is brought and may be properly maintained as a class action pursuant to Federal Rule of Civil Procedure 23.

64. Plaintiff brings this action on behalf of herself and all members of the following Class of similarly situated persons:

> All persons whose personally identifiable information and personal health information was accessed in the Data Breach by unauthorized persons, including all persons who were sent a notice of the Data Breach.

65. Plaintiff also brings this action on behalf of herself and all members of the following Subclass of similarly situated persons (the "GSK Subclass"):

> All persons whose personally identifiable information and personal health information was provided to GSK and was accessed in the Data Breach by unauthorized persons, including all such persons who were sent a notice of the Data Breach.

66. Excluded from the Class are Cencora, Inc., and its affiliates, parents, subsidiaries, officers, agents, and directors; The Lash Group, LLC, and its affiliates, parents, subsidiaries, officers, agents, and directors; GlaxoSmithKline, LLC, and its affiliates, parents, subsidiaries, officers, agents, and directors; GlaxoSmithKline Patient Access Programs Foundation, and its affiliates, parents, subsidiaries, officers, agents, and directors; as well as the judge(s) presiding over this matter and the clerks of said judge(s).

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

68. The members in the Class are so numerous that joinder of all Class members in a single proceeding would be impracticable. GSK reported to the Texas Attorney General's Office that 66,269 persons were affected by the Data Breach in Texas alone.[59]

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

a. whether Defendants had a duty to implement and maintain reasonable security procedures and practices to protect and secure Plaintiff's and Class members' PII/PHI from unauthorized access and disclosure;

b. whether Defendants had duties not to disclose the PII/PHI of Plaintiff and Class members to unauthorized third parties;

c. whether Defendants failed to exercise reasonable care to secure and safeguard Plaintiff's and Class members' PII/PHI;

d. whether an implied contract existed between Class members and GSK, providing that GSK would implement and maintain reasonable security measures to protect and secure Class members' PII/PHI from unauthorized access and disclosure;

e. whether Defendants engaged in unfair, unlawful, or deceptive practices by failing to safeguard the PII/PHI of Plaintiff and Class members;

f. whether Defendants breached their duties to protect Plaintiff's and Class members' PII/PHI; and

g. whether Plaintiff and Class members are entitled to damages and the measure of such damages and relief.

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

[59] *See Data Security Breach Report*, *supra* note 32.

71. Plaintiff's claims are typical of the claims of the Class. Plaintiff, like all proposed members of the Class, had her PII/PHI compromised in the Data Breach. Plaintiff and Class members were injured by the same wrongful acts, practices, and omissions committed by Defendants, as described herein. Plaintiff's claims therefore arise from the same practices or course of conduct that give rise to the claims of all Class members.

72. Plaintiff will fairly and adequately represent the interests of the Class members. Plaintiff has retained counsel with substantial experience and success in the prosecution of complex consumer protection class actions of this nature. Plaintiff has no interests adverse to, or that conflict with, the Class she seeks to represent. Plaintiff and her counsel have adequate resources to assure the interests of the Class will be adequately represented.

73. A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. The damages and other financial detriment suffered by Plaintiff and all other Class members are relatively small compared to the burden and expense that would be required to individually litigate their claims against Defendants, so it would be impracticable for Class members to individually seek redress from Defendants' wrongful conduct. Even if Class members could afford individual litigation, the court system could not. Individualized litigation creates a potential for inconsistent or contradictory judgments, and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court.

CAUSES OF ACTION

COUNT I
NEGLIGENCE

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

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

76. Defendants knew, or should have known, the risks of collecting and storing Plaintiff's and Class members' PII/PHI, and the importance of maintaining secure systems. Defendants knew, or should have known, of the many data breaches that targeted companies storing PII/PHI in recent years.

77. Given the nature of Defendants' business, the sensitivity and value of the PII/PHI they collect and maintain, and the resources at their disposal, Defendants should have identified the vulnerabilities in their systems and prevented the Data Breach from occurring.

78. Defendants breached these duties by failing to exercise reasonable care in safeguarding and protecting Plaintiff's and Class members' PII/PHI by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems to safeguard and protect PII/PHI entrusted to it—including Plaintiff's and Class members' PII/PHI.

79. It was, or should have been, reasonably foreseeable to Defendants that their failure to exercise reasonable care in safeguarding and protecting Plaintiff's and Class members' PII/PHI by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and

hardware systems would result in the unauthorized release, disclosure, and dissemination of Plaintiff's and Class members' PII/PHI to unauthorized individuals.

80. But for Defendants' negligent conduct or breach of the above-described duties owed to Plaintiff and Class members, their PII/PHI would not have been compromised.

81. As a result of Defendants' above-described wrongful actions, inaction, and want of ordinary care that directly and proximately caused the Data Breach, Plaintiff and all other Class members have suffered, and will continue to suffer, economic damages and other injury and actual harm in the form of, *inter alia*: (i) a substantially increased and imminent risk of identity theft and medical identity theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (ii) improper disclosure of their PII/PHI; (iii) breach of the confidentiality of their PII/PHI; (iv) deprivation of the value of their PII/PHI, for which there is a well-established national and international market; (v) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of medical identity theft they face and will continue to face; and (vi) overpayment for the services that were received without adequate data security.

COUNT II
NEGLIGENCE PER SE

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

83. Defendants' duties arise from, *inter alia*, the HIPAA Privacy Rule ("Standards for Privacy of Individually Identifiable Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and E, the HIPAA 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 (collectively, "HIPAA Privacy and Security Rules").

84. Defendants' duties also arise from Section 5 of the FTC Act ("FTCA"), 15 U.S.C. § 45(a)(1), which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted by the FTC, the unfair act or practice by businesses, such as Defendants, of failing to employ reasonable measures to protect and secure PII/PHI.

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

86. Defendants' violations of HIPAA Privacy and Security Rules and Section 5 of the FTCA, constitute negligence per se.

87. Plaintiff and Class members are within the class of persons that HIPAA Privacy and Security Rules and Section 5 of the FTCA were intended to protect.

88. The harm occurring as a result of the Data Breach is the type of harm HIPAA Privacy and Security Rules and Section 5 of the FTCA were intended to guard against.

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

90. The injury and harm that Plaintiff and the other Class members suffered was the direct and proximate result of Defendants' violations of HIPAA Privacy and Security Rules and Section 5 of the FTCA. Plaintiff and Class members have suffered (and will continue to suffer) economic damages and other injury and actual harm in the form of, *inter alia*: (i) a substantially increased and imminent risk of identity theft and medical identity theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (ii) improper disclosure of their PII/PHI; (iii) breach of the confidentiality of their PII/PHI; (iv) deprivation of the value of their PII/PHI, for which there is a well-established national and international market; (v) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of medical identity theft they face and will continue to face; and (vi) overpayment for the services that were received without adequate data security.

COUNT III
BREACH OF FIDUCIARY DUTY
Against GSK on Behalf of the GSK Subclass

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

92. Plaintiff brings this claim individually, and on behalf of the GSK Subclass, only against Defendants GlaxoSmithKline, LLC and GlaxoSmithKline Patient Access Programs Foundation.

93. Plaintiff and Class members gave GSK their PII/PHI in confidence, believing that GSK would protect that information. Plaintiff and Class members would not have provided GSK with this information had they known it would not be adequately protected. GSK' acceptance and storage of Plaintiff's and Class members' PII/PHI created a fiduciary relationship between GSK and Plaintiff and Class members. In light of this relationship, GSK must act primarily for the

benefit of their current and former patients or customers, which includes safeguarding and protecting Plaintiff's and Class members' PII/PHI.

94. GSK has a fiduciary duty to act for the benefit of Plaintiff and Class members upon matters within the scope of their relationship. It breached that duty by failing to, or contracting with companies that failed to, properly protect the integrity of the system containing Plaintiff's and Class members' PII/PHI, failing to comply with the data security guidelines set forth by HIPAA, and otherwise failing to safeguard Plaintiff's and Class members' PII/PHI that it collected and maintained.

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

COUNT IV
BREACH OF IMPLIED CONTRACT
Against GSK on Behalf of the GSK Subclass

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

97. Plaintiff brings this claim individually, and on behalf of the GSK Subclass, only against Defendants GlaxoSmithKline, LLC and GlaxoSmithKline Patient Access Programs Foundation.

98. In connection with receiving medical or healthcare services, Plaintiff and Class members entered into implied contracts with GSK.

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

100. The protection of PII/PHI was a material term of the implied contracts between Plaintiff and Class members, on the one hand, and GSK, on the other hand. Had Plaintiff and Class members known that GSK would not adequately protect their current and former patients' or customers' PII/PHI, they would not have sought healthcare services from GSK.

101. Plaintiff and Class members performed their obligations under the implied contract when they provided GSK with their PII/PHI and paid—directly or through their insurers—for health care or other services from GSK.

102. GSK breached their obligations under their implied contracts with Plaintiff and Class members in failing to implement and maintain reasonable security measures to protect and secure their PII/PHI and in failing to implement and maintain security protocols and procedures to

protect Plaintiff's and Class members' PII/PHI in a manner that complies with applicable laws, regulations, and industry standards.

103. GSK's breach of their obligations of their implied contracts with Plaintiff and Class members directly resulted in the Data Breach and the injuries that Plaintiff and all other Class members have suffered from the Data Breach.

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

COUNT V
UNJUST ENRICHMENT

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

106. This claim is pleaded in the alternative to the breach of implied contract claim.

107. Plaintiff and Class members conferred a monetary benefit upon Defendants in the form of monies paid to Defendants for healthcare services, either directly or indirectly, and through the provision of their PII/PHI.

108. Defendants accepted or had knowledge of the benefits conferred upon them by Plaintiff and Class Members. Defendants also benefitted from the receipt of Plaintiff's and Class members' PII/PHI, as this was used to facilitate payment.

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

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

111. Defendants should be compelled to provide for the benefit of Plaintiff and Class members all unlawful proceeds received by it as a result of the conduct and Data Breach alleged herein.

COUNT VI
VIOLATION OF THE NORTH CAROLINA UNFAIR AND DECEPTIVE TRADE PRACTICES ACT, N.C.G.S. §§ 75-1.1, *et seq.* ("NCUDTPA")
Against GSK on Behalf of the GSK Subclass

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

113. Plaintiff brings this claim individually, and on behalf of the GSK Subclass, only against Defendants GlaxoSmithKline, LLC and GlaxoSmithKline Patient Access Programs Foundation.

114. The NCUDTPA states, "Unfair methods of competition in or affecting commerce, and unfair or deceptive acts or practices in or affecting commerce, are declared unlawful." N.C.G.S. § 75-1.1(a).

115. The services that GSK provides are commerce within the meaning of N.C.G.S. § 75-1.1(a).

116. GSK made representations to Plaintiff and the Class members that their information would remain confidential, particularly in their Privacy Policy.

117. GSK did not disclose to Plaintiff and Class members that their data security was inadequate.

118. GSK violated the NCUDTPA through their failure to adequately safeguard and maintain Plaintiff and Class members' PII/PHI.

119. As a result of GSKs above-described conduct, Plaintiff and Class members have suffered damages from the disclosure of their information to unauthorized individuals.

120. The injury and harm that Plaintiff and the other Class members suffered was the direct and proximate result of GSK's violations of the NCUDTPA. Plaintiff and Class members have suffered (and will continue to suffer) economic damages and other injury and actual harm in the form of, *inter alia*: (i) a substantially increased risk of identity theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (ii) improper disclosure of their PII; (iii) breach of the confidentiality of their PII/PHI; (iv) deprivation of the value of their PII/PHI, for which there is a well-established national and international market; (v) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of identity theft they face and will continue to face; (vi) overpayment for the services that were received without adequate data security.

121. Plaintiff, individually, and for each member of the Class, seeks treble damages for their injuries pursuant to N.C.G.S. § 75-16 and attorneys' fees, litigation expenses and court costs pursuant to N.C.G.S. § 75-16.1.

PRAYER FOR RELIEF

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

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

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

C. Awarding Plaintiff and the Class equitable, injunctive, and declaratory relief, as may be appropriate. Plaintiff, on behalf of herself and the Class, seeks appropriate injunctive relief designed to prevent Defendants from experiencing another data breach by adopting and implementing best data security practices to safeguard PII/PHI and to provide or extend credit monitoring services and similar services to protect against all types of identity theft and medical identity theft;

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

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

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

JURY TRIAL DEMANDED

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

Respectfully submitted,

Dated: June 17, 2024

/s/ *Benjamin F. Johns*
Benjamin F. Johns
SHUB & JOHNS LLC
Samantha E. Holbrook
Andrea L. Bonner
200 Barr Harbor Dr., Suite 400
Conshohocken, PA 19428
Tel: 610-477-8380
bjohns@shublawyers.com
sholbrook@shublawyers.com
abonner@shublawyers.com

Ben Barnow*
Anthony L. Parkhill*
BARNOW AND ASSOCIATES, P.C.
205 West Randolph Street, Ste. 1630
Chicago, IL 60606
Tel: 312.621.2000
Fax: 312.641.5504
b.barnow@barnowlaw.com
aparkhill@barnowlaw.com

Attorneys for Plaintiff Barbara Buracker

**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

BARBARA BURACKER

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

(c) Attorneys *(Firm Name, Address, and Telephone Number)*
Benjamin F. Johns, Esq., Shub & Johns LLC, Four Tower Bridge, 200 Barr Harbor Drive, Suite 400, Conshohocken, PA 19428 Tel.: 610.477.8380. biohns@shublawyers.com

DEFENDANTS

CENCORA, INC., THE LASH GROUP, LLC, GLAXOSMITHKLINE, LLC, and GLAXOSMITHKLINE PATIENT ACCESS PROGRAMS FOUNDATION

County of Residence of First Listed Defendant Montgomery County, PA
(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

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

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

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. Rufe DOCKET NUMBER 2:24-cv-02227-CMR

DATE 6.17.2024

SIGNATURE OF ATTORNEY OF RECORD s/ Benjamin F. Johns

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: Pender County, North Carolina

Address of Defendant: 1 West First Avenue, Conshohocken, PA 19428-1800

Place of Accident, Incident or Transaction: 1 West First Avenue, Conshohocken, PA 19428-1800

RELATED CASE IF ANY:
Case Number: 2:24-cv-02227-CMR 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 17, 2024 _____ PA ID No. 201373

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, Benjamin F. Johns, 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 17, 2024 _____ PA ID No. 201373

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.