UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF NORTH CAROLINA

SARABETH EAVES and BONNIE EAVES, individually and on behalf of all others similarly situated, Plaintiffs, v. OCTAPHARMA PLASMA, INC. Defendant.	Case No. **CLASS ACTION COMPLAINT** JURY TRIAL DEMANDED

Plaintiffs Sarabeth Eaves and Bonnie Eaves ("Plaintiffs"), individually and on behalf of all others similarly situated (collectively, "Class members"), by and through their attorneys, bring this Class Action Complaint against Defendant Octapharma Plasma, Inc. ("Defendant" or "Octapharma") and complain and allege upon personal knowledge as to themselves and upon information and belief as to all other matters.

INTRODUCTION

1. This class action arises out of the recent targeted cyberattack and data breach that occurred on April 17, 2024, which affected Octapharma's inadequately protected computer systems and/or network, and which did result in the unauthorized access to Plaintiffs' and many other individuals' personally identifiable information ("PII") and personal health information ("PHI") (hereinafter the "Data Breach").

2. PII and PHI includes, among other sensitive information, confidential medical information, names, date of birth, addresses, payment card information, Social Security numbers ("SSNs"), medical record numbers, health plan beneficiary numbers, treatment information, diagnosis information, and/or other medical information.

3. Defendant is a global healthcare and pharmaceutical entity. Defendant develops and produces medicines based on the collection of human plasma. Defendant operates more than 195 plasma collection sites worldwide.

4. As a condition of receiving services, Defendant's patients are required to provide and entrust Defendant with sensitive and private information, including PII and PHI. By taking possession and control of patients' information, Defendant assumed a duty to implement adequate and reasonable cybersecurity procedures and protocols necessary to protect individuals PII and PHI from unauthorized disclosure.

5. Defendant also has a duty to adequately safeguard its patients sensitive and private information under industry standards and duties imposed by statutes, including the Health Insurance Portability and Accountability Act ("HIPPA") and Section 5 of the Federal Trade Commission Act ("FTC Act").

6. Defendant breached its duties by, among other things, failing to implement and maintain reasonable security procedures and practices to protect its patients' PII/PHI from unauthorized access and disclosure.

7. On April 17, 2024, Octapharma detected unauthorized activity within its computer systems and/or network and closed its plasma donation centers in the US while it investigated the incident to determine whether patient data was leaked as a result.[1] The breach affected Octapharma's network at 190 donation centers, spanning 35 US states.

8. Since its announcement of the Data Breach, Defendant has offered no assurance to Plaintiffs and Class Members that the sensitive and private information that was accessed in the Data Breach has been recovered or destroyed.

9. On or about April 24, 2024, the ransomware group known as BlackSuit took responsibility for the Data Breach, claiming that they stole sensitive PII and PHI from Octapharma's network. The stolen information was claimed to be 'patient names, Social Security

[1] https://www.octapharma.com/news/corporate-news/2024/news-update (last visited Apr. 29, 2024).

numbers, dates of birth, addresses, laboratory data, financial data, employee data, business data, and other data taken from shares and personal folders."[2]

10. The exposure of a person's PII and PHI through a data breach substantially increases that person's risk of identity theft, fraud, misappropriation of health insurance benefits, and similar forms of criminal mischief, potentially for the rest of their lives. Mitigation of such risk requires individuals to expend a significant amount of time and money to closely monitor their credit, financial accounts, health records, and email accounts. Mitigation of the risk of misuse of their sensitive and private information may not even be possible.

11. As a result of Defendant's inadequate security and breach of its duties and obligations, the Data Breach occurred, and Plaintiffs' and Class members' PII and/or PHI was accessed and disclosed. Plaintiffs and Class members are now at a substantially increased risk of experiencing misuse of their PII/PHI in the coming years. This action seeks to remedy these failings and their consequences.

12. Plaintiffs, on behalf of themselves and all other Class members whose PII/PHI was exposed in the Data Breach, assert claims for negligence, negligence per se, breach of fiduciary duty, breach of implied contract, and unjust enrichment, and seek declaratory relief, injunctive relief, monetary damages, statutory damages, punitive damages, equitable relief, and all other relief authorized by law.

PARTIES

13. Plaintiffs Sarabeth Eaves and Bonnie Eaves are citizens residing in Crandall, Georgia.

14. Plaintiffs are married are share assets, including, among others, bank accounts.

15. Plaintiffs were plasma donors of Defendant and were required to submit their personal information to Defendant as a condition of donating plasma, including their names, Social Security numbers, and full health and financial information.

[2] https://www.cyberdaily.au/security/10466-exclusive-black-suit-ransomware-gang-claims-hack-on-octapharma-plasma (last visited Apr. 29, 2024).

16. Defendant Octapharma Plasma, Inc. is a Delaware corporation with its headquarters in Charlotte, North Carolina.

JURISDICTION AND VENUE

17. This Court has subject matter jurisdiction pursuant to 28 U.S.C. § 1332, as emended by the Class Action Fairness Act of 2005, because the matter in controversy exceeds $5 million dollars, exclusive of interest and costs, and is a class action in which some members of the class are citizens of states different than Defendant. *See* 28 U.S.C. § 1332(d)(2)(A). This Court also has supplemental jurisdiction over the state law claims pursuant to 28 U.S.C. § 1367.

18. This Court has personal jurisdiction over Defendant because Defendant is headquartered in this District, regularly conducts business in this state, and the acts and omissions giving rise to Plaintiffs' claims emanated from within this District.

19. Venue is proper under 18 U.S.C. § 1391(b) because Defendant's headquarters is in this District, and a substantial part of the events or omissions giving rise to Plaintiffs' claims occurred in this District.

FACTUAL ALLEGATIONS

Defendant Stores Patient PII/PHI

20. Defendant is a global healthcare and pharmaceutical entity. Defendant develops and manufactures medicines from the collection of human plasma. It is the largest privately owned plasma fractionator in the world with locations in 31 countries.[3]

21. Defendant operates more than 195 plasma collection sites worldwide and. employs over 11,000 individuals throughout Europe and the United States.[4]

22. As a condition of collecting plasma from donors, Defendant requires that its donors entrust it with sensitive and private information such as their names, dates of birth, addresses, Social Security number, and financial information in the ordinary course of its business. Defendant also collects sensitive personal and health information such as PII/PHI.

[3] https://www.octapharmausa.com/about-us.
[4] https://www.octapharmausa.com/about-us/who-we-are.

Defendant collects and maintains the aforementioned information to provide medical services to donors.

23. Upon information and belief, the type of information that Defendant maintains includes, *inter alia*: patients' full name, address, date of birth, Social Security number ("SSN"), credit/debit card information, medical history, insurance information, billing information, medical records, photo identification, and any other information necessary to provide care.

24. Due to the highly sensitive nature of the information Defendant collects and maintains, Defendant is obligated provide confidentiality and adequate security for donor safety through its applicable privacy policy, and otherwise in compliance with statutory privacy requirements.

25. In the course of their relationship, Plaintiffs and Class Members provided Defendants with at least their PII and/or PHI.

26. Plaintiffs and Class Members, as current donors of Defendant, relied on Defendant to keep their sensitive PII/PHI confidential and secured, to use such information for business purposes only, and to make only authorized disclosures of this information.

The Data Breach

27. On or about April 17, 2024, Defendant detected unauthorized activity within its systems. In response, it launched an investigation into the source of the disruption.

28. Notably, Defendant has yet to publicly disclose the details of the attack, including when the breach occurred, or the full spectrum of information stolen. Defendant has simply told the public that the investigation was pending and that it hoped to open its plasma centers soon.

29. Defendant never confirmed that their investigation revealed that an unauthorized party gained access to files on its network that contained sensitive PII/PHI.

30. Yet the ransomware group "BlackSuit" took responsibility for the attack on or about April 24, 2024. The stolen information has been confirmed to include patients' sensitive PII

and/or PHI.[5]

31. Healthcare entities such as Defendant were notified by the US Department of Health and Human Services ("HHS") in November 2023 that the sector is at risk for an attack from Blacksuit.[6]

32. Based on the unfortunate events described throughout this Complaint, Defendant did not heed HHS' warning and failed to take action to prevent the Data Breach by implementing data security measures to protect its network from unauthorized breach.

33. Upon information and belief, the cyberattack was targeted at Defendant, due to its status as a healthcare entity that collects, creates, and maintains PII/PHI on its computer network and/or systems.

34. Plaintiffs' and Class Members' PII/PHI was compromised and acquired in the Data Breach.

35. Plaintiffs further believe that their PII/PHI was or soon will be published to the dark web, where it will be available to purchase, which is the *modus operandi* of cybercriminals.

36. Plaintiffs and Class Members now face a heightened and continued threat of identity theft and other types of criminal mischief resulting from the Data Breach.

37. Defendant has failed to provide Plaintiffs and Class Members with assurances that their sensitive information has not been stolen. Defendant has also failed to provide Plaintiffs and Class Members with identity theft countermeasures such as credit reports.

Defendant Knew that PII/PHI is Valuable to Cybercriminals and Failed to Take Action to Prevent its Theft

38. At all relevant times, Defendant knew, or should have known, that Plaintiffs' and Class Members' PII/PHI was a target for cybercriminals. Despite such knowledge, Defendant

[5] *See* supra n.2

[6] American Hospital Association, *HHS alerts health care sector to new ransomware threat* (Nov. 9, 2023), https://www.aha.org/news/headline/2023-11-09-hhs-alerts-health-care-sector-new-ransomware-threat.

failed to implement and maintain reasonable and appropriate data privacy and security measures to protect Plaintiffs' and Class members' PII/PHI from cyberattacks.

39. By acquiring, collecting, and using Plaintiffs' and Class Members PII/PHI, Defendant assumed legal and equitable duties created by the HIPPA, the FTCA, industry standards, contract, and common law to keep Plaintiffs' and Class Members PII/PHI confidential, and to protect it from unauthorized access and disclosure.

40. Additionally, Defendant's data security obligations were of particular importance due to the steady increase over the years of data breaches targeting medical information.

41. The healthcare industry is a known target for cyber criminals. "High demand for patient information and often-outdated systems are among the nine reasons healthcare is not the biggest target for online attacks."[7] They are also more likely to pay for a hacker's ransom due to the sensitive information that they maintain and collect, and an incentive to regain access to their data quickly.[8]

42. The number of data breaches experienced by healthcare entities continues to rise. In a 2024 report, the healthcare compliance company Protenus found that there were 942 medical data breaches in 2023, leaving over 171 million patient records exposed. This is an increase from the 905 medical data breaches that Protenus compiled in 2021.[9]

43. According to Mimecast, a cybersecurity firm, 90% of healthcare organizations experienced cyberattacks in 2020.[10]

---

[7] Swivel Secure, *The healthcare industry is at risk*, https://swivelsecure.com/solutions/healthcare/healthcare-is-the-biggest-target-for-cyberattacks/ (last visited Apr. 24, 2024).

[8] Elise Takahama, *Why health care has become a top target for cybercriminals*, The Seattle Times (Feb. 25, 2024), https://www.seattletimes.com/seattle-news/health/why-health-care-has-become-a-top-target-for-cybercriminals/. (last visited Apr. 26, 2024).

[9] *2024 Breach Barometer*, PROTENUS, https://www.protenus.com/breach-barometer-report (last visited Apr. 23, 2024).

[10] Maria Hernandez, *Iowa City Hospital Suffers Phishing Attack*, Security Magazine (Nov. 23, 2020), https://www.securitymagazine.com/articles/93988- iowa-city-hospital-suffers-phishing-attack (last visited April 29, 2024).

44. The last several years are marked by several high-profile healthcare data breaches including:

- Eastern Radiologists, Inc. (886,746 patients, February 2024);
- MCNA Dental (8,900,000 patients, March 2023);
- Broward Health (1,300,000 patients, January 2022);
- Morley (521,046 patients, February 2022);
- Regal Medical Group (3,300,000 patients, December 2022);
- Trinity Health (3,300,000 patients, March 2020);
- Shields Healthcare Group (2,000,000 patients, March 2022); and
- One Touch Point (2,600,000 individuals, July 2022).

45. An article from April 23, 2024 discussed the latest findings in Baker Hostetler's tenth annual Data Security Incident Response Report, which found that despite companies' adeptness to respond to cyberattacks from criminals, "ransomware attacks show no signs of abating…"[11] Moreover, "Combating these attacks has also been complicated by hackers' practice of constantly innovating and evolving their methods in order to get around the controls and safeguards that businesses are erecting to counter their attacks…"[12]

46. Defendant certainly knew and understood that unprotected or exposed PII/PHI in the custody of healthcare entities, like Defendant, is valuable and highly sought after by criminals seeking to illegally monetize that PII/PHI through unauthorized access.

47. Indeed, personal data such as PII/PHI is a valuable property right, leading to the purchase of said data by American companies. American companies have spent over $19 billion on acquiring personal data of consumers in 2018.[13]

---

[11] Allison Grande, *Ransomware Still on the Rise Despite Better Defenses, Firm Says*, LAW 360 (Apr. 23, 2024), https://www.law360.com/articles/1827647/ransomware-still-on-rise-despite-better-defenses-firm-says

[12] *Id.*

[13] *U.S. Firms to Spend Nearly $19.2 Billion on Third-Party Audience Data and Data-Use Solutions in 2018, Up 17.5% from 2017*, INTERACTIVE ADVERTISING BUREAU (Dec. 5, 2018), https://www.iab.com/news/2018-state-of-data-report/ (last visited Apr. 23, 2024).

48. Consumers also place a high value on the privacy of their data. 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."[14] Recently, more consumers are exercising their Data Subject Access Rights and leaving providers over their data practices and policies.[15]

49. Considering the value behind PII/PHI, 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.

50. PII/PHI is also of high value to identity thieves, as evidenced by their practice of trading such private information including, SSNs, on the black market or "dark web." PII/PHI is a measurable commodity on the black market.[16] PHI is particularly valuable and has been referred to as a "treasure trove for criminals."[17] In 2021, it was reported that stolen healthcare records can also fetch for as much as $1000 on the black market.[18] That price is likely much higher today.

[14] Janice Y. Tsai et al., *The Effect of Online Privacy Information on Purchasing Behavior, An Experimental Study*, 22(2) INFORMATION SYSTEMS RESEARCH 254 (June 2011), available for download at: https://www.jstor.org/stable/23015560?seq=1.

[15] CISCO, *Cisco 2023 Consumer Privacy Survey* (April 2023), available at https://www.cisco.com/c/en/us/about/trust-center/consumer-privacy-survey.html?CCID=cc000742

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

[17] *See* Andrew Steger, *What Happens to Stolen Healthcare Data?*, HEALTHTECH MAGAZINE (Oct. 30, 2019), https://healthtechmagazine.net/article/2019/10/what-happens-stolen-healthcare-data-perfcon (quoting Tom Kellermann, Chief Cybersecurity Officer, Carbon Black, stating "Health information is a treasure trove for criminals.") (last visited Apr. 23, 2024).

[18] Paul Nadrag, *Industry Voices-Forget credit card numbers. Medical records are the hottest items on the dark web*, FIERCE HEALTHCARE (Jan. 26, 2021), https://www.fiercehealthcare.com/hospitals/industry-voices-forget-credit-card-numbers-medical-records-are-hottest-items-dark-web (last visited Apr. 29, 2024).

51. According to a report released by the Federal Bureau of Investigation's ("FBI") Cyber Division, criminals can sell healthcare records for 50 times the price of a stolen Social Security or credit card number.[19]

52. Another report demonstrates that cybercriminals continue to profit from ransomware attacks: "The largest ransom paid in 2023 was more than $10 million, an increase from the $8 million payment high from 2022, and the average ransom paid in 2023 was $747,651, which nearly matches the average payment high that was set in 2020 during the height of the ransomware epidemic, the report noted."[20]

53. Companies like Defendant are aware that consumers value the privacy of their sensitive data such as PII/PHI and that cybercriminals continue to successfully target that data to obtain significant profits. As such, companies like Defendant remain on high alert and must act in accordance with their legal and equitable obligations to implement reasonable security measures to prevent targeted data attacks aimed at their patients' PII/PHI.

54. Armed with this knowledge, Defendant breached its duties by failing to implement and maintain reasonable security measures to protect Plaintiffs' and Class members' PII/PHI from being stolen.

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

55. The theft of PII/PHI is costly for those affected. A cybercriminal who steals a person's PHI can end up with as many as "seven to 10 personal identifying characteristics of an individual."[21] A study by Experian found that the "average total cost" of medical identity theft is

[19] *See Health Care Systems and Medical Devices at Risk for Increased Cyber Intrusions for Financial Gain*, FBI CYBER DIVISION (Apr. 8, 2014), https://www.illuminweb.com/wp-content/uploads/ill-mo-uploads/103/2418/health-systems-cyber-intrusions.pdf.

[20] *Supra* n.11.

[21] *Supra* n.17.

"about $20,000" per incident, and that a majority of victims of medical identity theft were forced to pay out-of-pocket costs for healthcare they did not receive in order to restore coverage.[22]

56. Identity thieves use personal information for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud. According to Experian, one of the largest credit reporting companies in the world, identity theft can happen in many ways: fraudsters can obtain and sell personal data to other criminals, or use personal data to open a new credit card or loan, open a bank account and write bad checks, apply for government benefits, take over existing debit and credit accounts, withdraw funds, and even get medical procedures.[23]

57. The Federal Trade Commission ("FTC") also warns consumers about the type of fraud that identity thieves use PII/PHI to achieve.[24] Criminals can also obtain a driver's license or official identification card in the victim's name, but with the thief's picture, use the victim's name and SSN to obtain government benefits, or filing a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's SSN, rent a house, or receive medical services in the victim's name, and may even give the victim's personal information to police during an arrest, resulting in an arrest warrant being issued in the victim's name.[25]

[22] Elinor Mills, *Study: Medical identity theft is costly for victims*, CNET (Mar. 3, 2010), https://www.cnet.com/news/study-medical-identity-theft-is-costly-for-victims (last visited Apr. 24, 2024).

[23] 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/ (last visited Apr. 25, 2024).

[24] *See What to Know About Identity Theft*, FEDERAL TRADE COMMISSION CONSUMER ADVICE, https://www.consumer.ftc.gov/articles/what-know-about-identity-theft (last visited Apr. 25, 2024).

[25] *See Warning Signs of Identity Theft*, FEDERAL TRADE COMMISSION, https://www.identitytheft.gov/Warning-Signs-of-Identity-Theft (last visited Apr. 25, 2024).

58. Alarmingly, a thief can use stolen medical information to extort a financial payment by "leveraging details specific to a disease or terminal illness."[26]

59. Identity theft is not an easy problem to solve. In a survey, the Identity Theft Resource Center found that most victims of identity crimes need more than a week to resolve issues stemming from identity theft and some need months to a year.[27]

60. Theft of SSNs also creates a particularly alarming situation for victims because those numbers cannot easily be replaced. To obtain a new number, a breach victim has to demonstrate ongoing harm from misuse of her SSN, and a new SSN will not be provided until after the harm has already been suffered by the victim.

61. Victims of medical identity theft face another set of problems. 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:

- 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;
- Significant bills for medical goods and services not sought nor received;
- Issues with insurance, co-pays, and insurance caps;
- Long-term credit problems based on problems with debt collectors reporting debt due to identity theft;
- Serious life consequences resulting from the crime; for example, victims have been falsely accused of being drug users based on falsified entries to their medical files; victims have had their children removed from them due to medical activities of the imposter; victims have been denied jobs due to incorrect information placed in their health files due to the crime;

[26] *Supra* n.17.

[27] Identity Theft Resource Center, 2023 Consumer Impact Report, available for download at: https://www.idtheftcenter.org/publications/

- 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;
- Phantom medical debt collection based on medical billing or other identity information; and
- Sales of medical debt arising from identity theft can perpetuate a victim's debt collection and credit problems, through no fault of their own.[28]

62. Further complicating victims' ability to defend themselves from identity theft is the time lag between when PII/PHI 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, and it takes some individuals up to three years to learn that information.[29]

63. Plaintiffs and Class members now live with their PII/PHI exposed in cyberspace and available to people willing to purchase and use the information for any number of improper purposes and crimes.

64. Plaintiffs and Class Members now face constant surveillance of their financial and personal records, monitoring, and loss of rights. Plaintiffs and Class Members are incurring and will continue to incur such damages, in addition to any fraudulent use of their PII/PHI.

Defendant Failed to Comply with Statutory Regulations

65. The Health Insurance Portability and Accountability Act ("HIPPA") requires covered entities to implement reasonable security measures to protect patient information, including protected health information, defined as "individually identifiable health information" which either "identifies the individual" or where there is a "reasonable basis to believe the information can be used to identify the individual," that is held or transmitted by a healthcare provider. *See* 45 C.F.R. § 160.103.

[28] World Privacy Forum, *The Geography of Medical Identity Theft* (Dec. 12, 2017), available for download at: https://www.worldprivacyforum.org/2017/12/new-report-the-geography-of-medical-identity-theft/

[29] John W. Coffey, *Difficulties in Determining Data Breach Impacts*, 17 JOURNAL OF SYSTEMICS, CYBERNETICS AND INFORMATICS 9 (2019), http://www.iiisci.org/journal/pdv/sci/pdfs/IP069LL19.pdf

66. HIPPA further prohibits the unauthorized disclosure of protected health information.

67. Defendant is a HIPPA covered entity that provides healthcare services. *See* 45 C.F.R. § 160.12. As a regular and necessary part of its business, Defendant collects and maintains PII/PHI of patients.

68. HIPPA requires Defendant to implement adequate safeguards to prevent unauthorized use or disclosure of private information such as PII/PHI by adopting the requirements set forth in the HIPPA's Privacy Rule and Security Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and E ("Standards for Privacy of Individually Identifiable Health Information), and Security Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and C ("Security Standards for the Protection of Electronic Protected Health Information").

69. Defendant is also required to report any unauthorized use or disclosure of that information, including incidents of a data breach "without unreasonable delay and in no case later than 60 days following discovery of the breach."[30] *See* 45 C.F.R. § 164.302.

70. As a HIPPA covered entity, Defendant assumed legal obligations and knew or should have known that it was responsible for safeguarding Plaintiffs' and Class Members sensitive and private information from unauthorized disclosure.

71. As set forth throughout this Complaint, Defendant did not implement the required safeguards it is required to maintain under HIPPA. Defendant did so with knowledge of its legal duties under HIPPA and of the risks associated with unauthorized access to Plaintiffs' and Class Members' PHI.

72. Defendant's HIPPA violations include but are not limited to the following:

a. Failing to ensure the confidentiality and integrity of electronic PHI that it creates, receives, maintains and transmits. 45 C.F.R. § 164.306(a)(1);

b. Failing to protect against any reasonably-anticipated threats or hazards to the security or integrity of PHI. 45 C.F.R. § 164.306(a)(2);

[30] Breach Notification Rule, U.S. Dep't of Health & Human Services, https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html

c. Failing to protect against any reasonably anticipated uses or disclosure of electronic PHI that is not permitted. 45 C.F.R. § 164.306(a)(3);

d. Failing to ensure compliance with HIPPA security standards by Defendant's workforce. 45 C.F.R. § 164.306(a)(4);

e. Failing to implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights. 45 C.F.R. § 164.312(a)(1);

f. Failing to implement policies and procedures to prevent, detect, contain and correct security violations. 45 C.F.R. § 164.308(a)(1);

g. Failing to identify and respond to suspected or known security incidents and failing to mitigate the harmful effects of security incidents that are known. 45 C.F.R. § 164.308(a)(6)(ii);

h. Failing to effectively train all staff members on the policies and procedures with respect to PHI as necessary and appropriate for staff members to carry our their functions and to maintain security of PHI. 45 C.F.R. § 164.530(b); 45 C.F.R. § 164.308(a)(5); and

i. Failing to design, implement, and enforce policies and procedures establishing physical and administrative safeguards to reasonably safeguard PHI. 45 C.F.R. § 164.530(c).

73. As a result of their failure to comply with HIPPA regulations, cybercriminals circumvented Defendant's lax security measures, resulting in the Data Breach and injuring Plaintiffs and Class Members.

74. The Federal Trade Commission Act ("FTCA") prohibits Defendant from engaging in "unfair or deceptive acts or practices in or affecting commerce." *See* 15 U.S.C. § 45.

75. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses which reflect the importance of implementing reasonable data security practices.

76. The FTC's publication, Protecting Personal Information, established cyber-security guidelines for businesses. The guidelines provide that businesses should take action to protect the personal patient information that they collect; properly dispose of personal information

that is no longer needed; encrypt information stored on computer networks; understand their networks' vulnerabilities; and implement policies to correct any security problems.[31]

77. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[32]

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

79. The FTC has the authority to bring enforcement actions against businesses for failing to protect PII/PHI adequately and reasonably under Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45.

80. The orders that result from enforcement actions further clarify the measures businesses must take to meet their data security obligations.

81. Defendant failed to properly implement basic data security practices.

82. Defendant was at all relevant times fully aware of its obligations to protect donors' PII/PHI, and of the significant consequences that would result from its failure to do so.

83. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to donors' PII/PHI constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

[31] Protecting Personal Information: A Guide for Business, Federal Trade Commission (2016). Available at https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business.

[32] *Id.*

84. Consequently, cybercriminals circumvented Defendant's lax security measures, resulting in the Data Breach.

Defendant Failed to Comply with Industry Standards

85. Industry standards for healthcare providers such as Defendant exist because of the high threat of cyberattacks that target the sensitive information that they collect and maintain.

86. These practices include, but are not limited to: educating and training employees about the risks of cyberattacks, strong passwords, multi-layer security such as firewalls, anti-virus and malware software, encryption, multi-factor authentication, backup data, limitation of employees with access to sensitive data, setting up network firewalls, switches and routers, monitoring and limiting the network ports, and monitoring and limited access to physical security systems.

87. Defendant failed to meet the minimum standards of any of the following: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

88. The Defendant's failure to implement the industry standards described herein resulted in the Data Breach and caused injury to Plaintiffs and Class Members.

Common Damages Sustained by Plaintiffs and Class Members

89. For the reasons mentioned above, Plaintiffs and all other Class members have suffered injury and damages directly attributable to Defenant's failure to implement and maintain adequate security measures, including, but not limited to: (i) fraudulent bank accounts opened in their names (ii) a substantially increased risk of identity theft and medical theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (iii) improper disclosure of their PII/PHI; (iii) breach of the confidentiality of their PII/PHI; (iv) invasion of their privacy; (v) deprivation of the value of their PII/PHI, for which there is a well-

established national and international market; and/or (vi) lost time and money incurred to mitigate 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.

Plaintiffs' Experience

90. Plaintiffs Sarabeth Eaves and Bonnie Eaves are a married couple and current plasma donors of Defendant.

91. As a condition of donating plasma to Defendant, Plaintiffs were required to provide private information to Defendant including their names, Social Security numbers, and full health and financial information.

92. Upon information and belief, Defendant retained Plaintiffs' private information in its system at the time of the Data Breach.

93. Plaintiffs are careful about sharing their private information. Plaintiffs store any documents containing private information in a safe and secure location. Plaintiffs would not have entrusted their private information with Defendant had they known of Defendant's failure to implement and maintain data security measures.

94. Plaintiffs' PII and/or PHI was improperly accessed and obtained by unauthorized third parties in the Data Breach.

95. Since the announcement of the Data Breach, Plaintiffs have been required to spend valuable time monitoring their various accounts in an effort to detect and prevent any misuses of their PII/PHI, time they would not have had to spend but for the Data Breach.

96. Indeed, around the time of the Data Breach, Plaintiffs received notification from their bank that two unauthorized bank accounts were opened in their name, thereby heightening the need for them to spend time to carefully monitor the fraud.

97. As a result of the Data Breach, Plaintiffs suffered actual injury including, but not limited to: (i) fraudulent bank accounts opened in their names; and (ii) a substantially increased risk of identity theft and medical theft; (iii) improper disclosure of their PII/PHI; (iii) breach of the confidentiality of their PII/PHI; (iv)

invasion of their privacy; (v) deprivation of the value of their PII/PHI, for which there is a well-established national and international market; and/or (vi) lost time and money incurred to mitigate 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.

98. The Data Breach has caused Plaintiffs to suffer fear, anxiety, and stress, which is amplified by the fact that key details about the Data Breach are still unknown, and Plaintiffs' PII/PHI is still at risk of being stolen and used for fraudulent activity.

CLASS ALLEGATIONS

99. Plaintiffs bring this class action individually and on behalf of all persons similarly situated, pursuant to Federal Rules of Civil Procedure 23(a), 23(b)(1), 23(b)(2), and 23(b)(3).

100. Plaintiffs seek certification of a Class as defined below and subject to further amendment:

Nationwide Class

All individuals in the United States whose PII and/or PHI was compromised in the Data Breach that was announced April 17, 2024 (the "Class").

101. Excluded from the Class is Defendant 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).

102. Certification of Plaintiffs' claims for class-wide treatment is appropriate because Plaintiffs can prove the elements of his 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.

103. Numerosity. The members in the Class are so numerous that joinder of all Class members in a single proceeding would be impracticable. While the exact number of individuals affected is unknown, Defendant reported that the Data Breach has affected 190 plasma donation centers across 35 states, potentially affecting thousands of individuals. The contact information of those individuals are available from Defendant's business records.

104. Commonality. 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 Defendant had a duty to implement and maintain reasonable security procedures and practices to protect and secure Plaintiffs' and Class Members' PII/PHI from unauthorized access and disclosure;

b. Whether Defendant failed to exercise reasonable care to secure and safeguard Plaintiffs' and Class Members' PII/PHI;

c. Whether Defendant breached its duties to protect Plaintiffs' and Class members' PII/PHI;

d. Whether defendant breached its fiduciary duty to Plaintiffs and Class Members;

e. When Defendant learned of the Data Breach;

f. Whether Defendant knew or should have known that its data security systems and monitoring procedures were deficient;

g. Whether hackers obtained Plaintiffs' and Class Members' data in the Data Breach;

h. Whether an implied contract existed between Class members and Defendant providing that Defendant would implement and maintain reasonable security measures to protect and secure Class Members' PII/PHI from unauthorized access and disclosure;

i. Whether Defendant was unjustly enriched;

j. Whether Defendant's conduct violates various states' consumer protection statutes;

k. Whether Plaintiffs and Class Members are entitled to injunctive relief and identity theft protection to redress the imminent harm they face due to the Data Breach; and

l. Whether Plaintiffs and all other members of the Class are entitled to damages and the measure of such damages and relief.

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

106. Adequacy of Representation. Plaintiffs will fairly and adequately protect the interests of the Class members. Plaintiffs are adequate representatives of the Class in that they have no interests adverse to, or conflict with, the Class they seek to represent. Plaintiffs have retained counsel with substantial experience and success in the prosecution of complex consumer protection class actions of this nature.

107. Superiority. A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. The damages and other financial detriment suffered by Plaintiffs and all other Class members are relatively small compared to the burden and expense that would be required to individually litigate their claims against Defendant, so it would be impracticable for Class members to individually seek redress from Defendant's 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.

108. All members of the proposed Class are readily ascertainable. Defendant has access to the names, addresses, and/or email addresses of Class Members affected by the Data Breach.

109. Finally, class certification is appropriate under Fed. R. Civ. P. 23(b). Defendant engaged in a common course of conduct giving rise to the legal rights sought to be enforced by

Plaintiffs on behalf of themselves 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.

CAUSES OF ACTION

COUNT I
NEGLIGENCE
(Plaintiffs, on behalf of themselves and the Nationwide Class)

110. Plaintiffs reallege and incorporate by reference all preceding paragraphs as if fully set forth herein.

111. Defendant requires that its donors, including Plaintiffs and Class Members, submit private information such as PII and PHI in the course of providing its medical services.

112. Defendant collected, acquired, and stored Plaintiffs and Class Members' private information.

113. Plaintiffs and Class Members entrusted Defendant with their private information and had the understanding that Defendant would safeguard their information.

114. Defendant had knowledge of the sensitivity of Plaintiffs and Class Members' private information, and the consequences that would result from the unauthorized disclosure of such information. Defendant knew that healthcare entities were the target of cyberattacks in the past, and that Plaintiffs and Class members were the foreseeable and probable victims of any inadequate data security procedures.

115. It was therefore reasonably foreseeable that the failure to implement adequate data security procedures would result in injuries to the Plaintiffs and Class Members.

116. Defendant owed a duty to Plaintiffs and Class members to exercise reasonable care in safeguarding and protecting their private information in its possession, custody, or control from the unauthorized disclosure of such information.

117. Defendant's duty to exercise reasonable care arises from several sources, including but not limited to common law, the HIPPA, the FTCA, and industry standards.

118. Defendant's duty also arose from its position as a healthcare provider. As a healthcare provider, Defendant assumed a duty to exercise reasonable care in safeguarding and protecting donors' private information in its possession, custody, or control from the unauthorized disclosure of such information.

119. Defendant breached its duty by failing to exercise reasonable care in safeguarding and protecting Plaintiffs' 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 Plaintiffs' and Class members' PII/PHI.

120. Defendant admitted that the PII/PHI of Plaintiffs and Class Members was disclosed to unauthorized third persons as a result of the Data Breach.

121. Defendant's negligent conduct or breach of the above-described duties owed to Plaintiffs and Class members caused their PII/PHI to be compromised in the Data Breach.

122. Plaintiffs and Class Members were in no position to protect their PII/PHI themselves.

123. But for Defendant's breach of the duties described herein, Plaintiffs and Class Members' PII and PHI would not have been compromised.

124. There is a causal relationship between Defendant's failure to implement, control, direct, oversee, manage, monitor, and audit adequate data security procedures to protect the PII and PHI of its donor and the harm suffered by Plaintiffs and Class Members.

125. As a direct and proximate result of Defendant's conduct described above, it directly and proximately caused the Data Breach, and Plaintiffs and all other Class members have suffered, and will continue to suffer, economic damages and other injury and actual harm in the form of, *inter alia*: (i) a substantially increased risk of identity theft and medical theft—risks justifying expenditures for protective and remedial services for which they are entitled to

compensation; (ii) actual identity theft; (iii) improper disclosure of their PII/PHI; (iv) breach of the confidentiality of their PII/PHI; (v) deprivation of the value of their PII/PHI, for which there is a well-established national and international market; and/or (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.

126. As a direct and proximate result of Defendant's wrongful conduct, Plaintiffs and Class Members have suffered and will continue to suffer other forms of injury, including but not limited to, anxiety, emotional distress, invasion of privacy, and other economic and non-economic losses.

127. Plaintiffs and Class members are entitled to damages incurred as a result of the Data Breach.

128. Defendant's negligent conduct is ongoing, in that it still holds Plaintiffs' and Class Members PII and/or PHI in an unsafe and insecure manner.

129. Plaintiffs and Class Members are also entitled to injunctive relief in the form of requiring Defendant to strengthen its data security procedures and to provide credit monitoring to Class Members.

COUNT II
NEGLIGENCE PER SE
(Plaintiffs, on behalf of themselves and the Nationwide Class)

130. Plaintiffs reallege and incorporate by reference all preceding paragraphs as if fully set forth herein.

131. Defendant's 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, and 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").

132. Defendant's 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 a business, such as Defendant of failing to employ reasonable measures to protect and secure PII/PHI.

133. Defendant violated HIPAA Privacy and Security Rules, Section 5 of the FTCA, UCL, CMIA, and CCPA by failing to use reasonable measures to protect Plaintiffs' and Class Members' PII/PHI and not complying with applicable industry standards. Defendant's 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 Plaintiffs and the other Class members.

134. Defendant's violations of HIPAA Privacy and Security Rules and Section 5 of the FTCA constitutes negligence *per se*.

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

136. 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.

137. It was reasonably foreseeable to Defendant that its failure to exercise reasonable care in safeguarding and protecting Plaintiffs' 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 Plaintiffs' and Class members' PII/PHI to unauthorized individuals.

138. The injury and harm that Plaintiffs and the other Class members suffered were the direct and proximate result of Defendant's violations of HIPAA Privacy and Security Rules, and Section 5 of the FTCA. Plaintiffs and Class members have suffered (and will continue to suffer) economic damages and other injury and actual harm in the form of, *inter alia*: (i) a

substantially increased risk of identity theft and medical theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (ii) actual identity theft; (iii) improper disclosure of their PII/PHI; (iv) breach of the confidentiality of their PII/PHI; (v) deprivation of the value of their PII/PHI, for which there is a well-established national and international market; and/or (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.

139. As a direct and proximate result of Defendant's wrongful conduct, Plaintiffs and Class Members have suffered and will continue to suffer other forms of injury, including but not limited to, anxiety, emotional distress, invasion of privacy, and other economic and non-economic losses.

140. Plaintiffs and Class members are entitled to damages incurred as a result of the Data Breach.

141. Plaintiffs and Class Members are also entitled to injunctive relief in the form of requiring Defendant to strengthen its data security procedures and to provide credit monitoring to Class Members.

COUNT III
BREACH OF FIDUCIARY DUTY
(Plaintiffs, on behalf of themselves and the Nationwide Class)

142. Plaintiffs reallege and incorporate by reference all preceding paragraphs as if fully set forth herein.

143. Plaintiffs and Class members gave Defendant their PII/PHI in confidence, believing that Defendant would protect that information. Plaintiffs and Class members would not have provided Defendant with this information had they known it would not be adequately protected. Defendant's acceptance and storage of Plaintiffs' and Class Members' PII/PHI created a fiduciary relationship between Defendant and Plaintiffs and Class members. In light

of this relationship, Defendant must act primarily for the benefit of its donors, which includes safeguarding and protecting Plaintiffs' and Class Members' PII/PHI.

144. Defendant has a fiduciary duty to act for the benefit of Plaintiffs and Class Members upon matters within the scope of their relationship. It breached that duty by failing to properly protect the system containing Plaintiffs' and Class Members' PII/PHI, failing to comply with the data security guidelines set forth by HIPAA and the FTCA, and otherwise failing to safeguard Plaintiffs' and Class members' PII/PHI that it collected.

145. As a direct and proximate result of Defendant's breaches of its fiduciary duties, Plaintiffs and Class members have suffered and will suffer injury, including, but not limited to: (i) a substantially increased risk of identity theft and medical theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (ii) actual identity theft; (iii) improper disclosure of their PII/PHI; (iv) breach of the confidentiality of their PII/PHI; (v) deprivation of the value of their PII/PHI, for which there is a well-established national and international market; and/or (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.

146. As a direct and proximate result of Defendant's wrongful conduct, Plaintiffs and Class Members have suffered and will continue to suffer other forms of injury, including but not limited to, anxiety, emotional distress, invasion of privacy, and other economic and non-economic losses.

147. Plaintiffs and Class members are entitled to damages incurred as a result of the Data Breach.

148. Plaintiffs and Class Members are also entitled to injunctive relief in the form of requiring Defendant to strengthen its data security procedures and to provide credit monitoring to Class Members.

COUNT IV
BREACH OF IMPLIED CONTRACT

(Plaintiffs, on behalf of themselves and the Nationwide Class)

149. Plaintiffs reallege and incorporate by reference all preceding paragraphs as if fully set forth herein.

150. In connection with donating plasma or other medical services, Plaintiffs and all other Class members entered into implied contracts with Defendant or were intended third-party beneficiaries of contracts between Defendant and others.

151. Pursuant to these implied contracts, plasma was paid to Defendant, whether directly from Plaintiffs and Class members, and Defendant was provided with PII/PHI of Plaintiffs and Class members. In exchange, Defendant impliedly agreed to, among other things, take reasonable measures to protect the security and confidentiality of Plaintiffs' and Class members' PII/PHI; and protect Plaintiffs' and Class members PII/PHI in compliance with federal and state laws and regulations and industry standards.

152. The protection of PII/PHI was a material term of the implied contracts that were either between Plaintiffs and Class members, on the one hand, and Defendant, on the other hand or were between third parties and Defendant to which Plaintiffs and Class members were intended third party beneficiaries.

153. Plaintiffs and Class members or the third parties fulfilled their obligations under the contracts.

154. Defendant breached its obligations by failing to implement and maintain reasonable data security measures to protect and secure the PII/PHI and in failing to implement and maintain security protocols and procedures to protect Plaintiffs' and Class members' PII/PHI in a manner that complies with applicable laws, regulations, and industry standards.

155. Defendant's breach of its obligations of its implied contracts directly resulted in the Data Breach and the injuries that Plaintiffs and all other Class members have suffered from the Data Breach.

156. Plaintiffs and all other Class members were damaged by Defendant'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 of identity theft and medical theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (iii) they suffered actual identity theft; (iv) their PII/PHI was improperly disclosed to unauthorized individuals; (v) the confidentiality of their PII/PHI has been breached; (vi) they were deprived of the value of their PII/PHI, for which there is a well-established national and international market; and/or (vii) they lost time and money 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.

COUNT V
UNJUST ENRICHMENT
(Plaintiffs, on behalf of themselves and the Nationwide Class)

157. Plaintiffs reallege and incorporate by reference all preceding paragraphs as if fully set forth herein.

158. This count is pleaded in the alternative to Plaintiffs' breach of implied contract claim (Count IV).

159. Plaintiffs and Class members conferred a monetary benefit upon Defendant in the form of plasma paid to Defendant and/or its agents for healthcare services or other services.

160. In exchange, Plaintiffs and Class Members should have received from Defendant the services that were the subject of the transaction and should have had their private information protected with adequate data security procedures.

161. Defendant accepted or had knowledge of the benefits conferred upon it by Plaintiffs and Class Members by acquiring and/or collecting their private information as well as blood plasma made on their behalf as a necessary part of obtaining Defendant's services. Defendant appreciated and benefitted from the receipt of Plaintiffs' and Class members' private information and payments in that they used the private information and profited from the healthcare transactions in furtherance of its business.

162. Defendant acquired Plaintiffs' and Class Members' private information and payments through inequitable means in that it failed to disclose the inadequate data security procedures previously alleged herein.

163. As a result of Defendant's conduct, Plaintiffs 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 Plaintiffs and Class members paid for, and those payments without reasonable data privacy and security practices and procedures that they received.

164. Defendant should not be permitted to retain the PII/PHI belonging to Plaintiffs and Class members because Defendant failed to adequately implement the data privacy and security procedures for itself that Plaintiffs and Class members paid for and that were otherwise mandated by federal, state, and local laws and industry standards.

165. Defendant unjustly enriched itself by using the plasma and private information acquired by Plaintiffs and Class Members to further its business.

166. Notably, Defendant chose not to use any payments to enhance their data security procedures.

167. Under principles of equity and good conscience, Defendant should not be permitted to retain the money wrongfully obtained from Plaintiffs and Class Members, and be compelled to provide for the benefit of Plaintiffs and Class members, all unlawful proceeds received by it as a result of the conduct and Data Breach alleged herein.

PRAYER FOR RELIEF

Plaintiffs, individually and on behalf of all other members of the Class, respectfully request that the Court enter judgment in their favor and against Defendant as follows:

A. Certifying the Class as requested herein, designating Plaintiffs as Class representatives, and appointing Plaintiffs' counsel as Class Counsel;

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

C. Awarding Plaintiffs and the Class equitable, injunctive, and declaratory relief, as may be appropriate. Plaintiffs, on behalf of themselves and the Class, seek appropriate injunctive relief designed to prevent Defendant 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 Plaintiffs and the Class pre-judgment and post-judgment interest to the maximum extent allowable;

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

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

JURY TRIAL DEMANDED

Plaintiffs demand a trial by jury of all claims in this Class Action Complaint so triable.

Dated: April 30, 2024

Respectfully submitted,

By: *s/ Jean S. Martin*
Jean S. Martin
MORGAN & MORGAN
COMPLEX LITIGATION GROUP
201 N. Franklin Street, 7th Floor
Tampa, Florida 33602
Telephone: (813) 223-5505
Facsimile: (813) 223-5402
jeanmartin@forthepeople.com

Steven A. Schwartz*
steveschwartz@chimicles.com
Beena M. McDonald*
bmm@chimicles.com
Alex M. Kashurba*

amk@chimicles.com
Marissa N. Pembroke*
mnp@chimicles.com
CHIMICLES SCHWARTZ KRINER & DONALDSON-SMITH LLP
One Haverford Centre
361 Lancaster Avenue
Haverford, PA 19041
Telephone: (610) 642-8500

**pro hac vice* to be submitted

Counsel for Plaintiffs and the Proposed Class

JS 44 (Rev. 03/24)

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

SARABETH EAVES and BONNIE EAVES, individually and on behalf of all others similarly situated,

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

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

Morgan and Morgan Complex Litigation Group, 201 N. Franklin St, 7th Fl, Tampa, Fl 33602 Tel: (813) 223-5505

DEFENDANTS

OCTAPHARMA PLASMA, INC.

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

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

Attorneys *(If Known)*

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

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

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

(For Diversity Cases Only)

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

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

Click here for: Nature of Suit Code Descriptions.

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

TORTS

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

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

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

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)***:
15 U.S.C. § 45, 42 U.S.C. § 17921, 42 U.S.C. § 17902, 28 U.S.C. §§ 2201

Brief description of cause:
Negligence, Negligence Per Se, Unjust Enrichment, Breach of Fiduciary Duty, Declaratory judgement/Injunctive Relief

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 _____ DOCKET NUMBER _____

DATE: Apr 30, 2024

SIGNATURE OF ATTORNEY OF RECORD: /s/ Jean Sutton Martin

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 cases, if any. If there are related cases, insert the docket numbers and the corresponding judge names for such cases.

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