UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF PENNSYLVANIA

WENDY MARSHALL, individually and on behalf of all others similarly situated, Plaintiff, v. HIGHMARK, INC., a Pennsylvania Corporation, Defendant.	**CIVIL ACTION NO.** 2:23-CV-290 **CLASS ACTION** **[JURY TRIAL DEMANDED]**

CLASS ACTION COMPLAINT

Plaintiff Wendy Marshall ("Plaintiff"), individually and on behalf of all others similarly situated, brings this Class Action Complaint and alleges the following against Defendant Highmark Inc. ("Highmark" or "Defendant"), based upon personal knowledge with respect to Plaintiff and upon information and belief derived from, among other things, investigation of counsel and review of public documents as to all other matters:

NATURE OF THE ACTION

1. This class action arises out of the recent data breach (the "Data Breach") involving Highmark, which collected and stored certain personally identifiable information ("PII") and/or protected health information ("PHI") of the Plaintiff and the putative Class Members, all of whom have PII/PHI on Highmark servers.

2. According to Highmark, the PII/PHI compromised in the Data Breach included highly-sensitive information including but not limited to: names, Social Security numbers, and may include enrollment information such as group names, identification numbers, claims or treatment information such as claim numbers, dates of service, procedures, prescription

information as well as in some cases financial information, addresses, and email addresses.[1]

3. Social Security numbers are particularly valuable to criminals. This information can be sold and traded on the dark web black market. The loss of a Social Security number is particularly troubling because it cannot be easily changed and can be misused in a range of nefarious activities, such as filing fraudulent tax returns to steal tax refund payments, opening new accounts to take out loans, and other forms of identity theft.

4. The Data Breach was a direct result of Defendant's failure to implement adequate and reasonable cybersecurity procedures and protocols necessary to protect consumers' PII/PHI. Inexplicitly, the Defendant has acknowledged that the cybersecurity attack occurred in December 15, 2022, but it has only recently begun contacting Class Members.

5. According to the Office of the Maine Attorney General, whom Defendant was required to notice, the Data Breach has affected 300,000 individuals.[2]

6. Plaintiff brings this class action lawsuit on behalf of Plaintiff individually as well as all those similarly situated to address Defendant's inadequate safeguarding of Class Members' PII/PHI that they collected and maintained, and for failing to provide timely and adequate notice to Plaintiff and other Class Members that their information was unsecured and left open to the unauthorized access of any unknown third party.

PARTIES

7. Plaintiff Wendy Marshall is an adult individual and citizen of the State of West Virginia who resides in Weirton, West Virginia. Plaintiff was a client of Defendant, which is a

[1] https://www.highmark.com/newsroom/press-releases/highmark-notifies-members-about-data-breach/ (last accessed February 7, 2023).
[2] https://apps.web.maine.gov/online/aeviewer/ME/40/67bb2ced-9a70-4248-b728-68a92a56c860.shtml (last accessed February 7, 2023).

national healthcare organization.

8. On or around February 13, 2023, Plaintiff Marshall was notified by Defendant via letter of the Data Breach and of the impact to their PII/PHI.

9. As a result of Defendant's conduct, Plaintiff Marshall suffered actual damages including, without limitation, time and expenses related to monitoring their financial accounts for fraudulent activity, facing an increased and imminent risk of fraud and identity theft, the lost value of their personal information, and other economic and non-economic harm. Plaintiff and Class Members will now be forced to expend additional time to review their credit reports and monitor their financial accounts and medical records for fraud or identify theft – particularly since the compromised information may include Social Security numbers.

10. Defendant Highmark Inc. is an entity that is a national healthcare organization, with its principal place of business and headquarters at 120 Fifth Ave Place, Suite 2114, Pittsburgh, PA 15222.

JURISDICTION AND VENUE

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

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

13. Defendant is headquartered and routinely conducts business in the Commonwealth where this district is located, has sufficient minimum contacts in this Commonwealth, and has

intentionally availed itself of this jurisdiction by marketing and selling products and services, and by accepting and processing payments for those products and services within this State.

14. Venue is proper in this Court under 28 U.S.C. §1391 because a substantial part of the events that gave rise to Representative Plaintiff's claims took place within this District, and Defendant does business in this Judicial District.

COMMON FACTUAL ALLEGATIONS

15. Plaintiff Marshall and the proposed Class are consumers of Defendant. Defendant Highmark is a national healthcare organization.[3]

16. As noted above, Plaintiff brings this class action against Defendant for Defendant's failure to properly secure and safeguard personally identifiable information, for failing to comply with industry standards to protect and safeguard that information, and for failing to provide timely, accurate, and adequate notice to Plaintiff and other members of the class that such information had been compromised.

Highmark's Unsecure Data Management and Disclosure of Data Breach

17. Plaintiff and Class Members provided their PII/PHI to Defendant with the reasonable expectation and mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access.

18. Plaintiff and Class Members' PII/PHI was provided to Defendant in conjunction with the type of work Defendant does within the healthcare industry and as an independent licensee of the Blue Cross Blue Shield Association.[4]

---

[3] https://www.highmark.com/newsroom/press-releases/highmark-notifies-members-about-data-breach/ (last accessed February 7, 2023).

[4] *See id.*

19. However, Defendant failed to secure the PII/PHI of the individuals that provided it with this sensitive information.

20. Defendant's data security obligations were particularly important given the substantial increase in cyber-attacks and/or data breaches preceding the date they disclosed the incident.

21. According to Defendant, an incident occurred between December 13, 2022 and December 15, 2022, "whereby an employee was sent a malicious phishing email link that led to their email account being compromised and a threat actor obtained access to files that may have contained the protected health information (PHI) of Highmark members.[5]

22. Defendant stated it "immediately respondent to this incident and launched an investigation," and took actions including "contain[ing] the mailbox, remov[ing] the malicious email from all domain users, and implement[ing] additional preventative and monitoring controls."[6]

23. Defendant "also engaged a third-party digital forensics firm to determine the full extent of the breach," and allegedly "takes the security of member information seriously and has implemented a robust action plan to bolster employee training on phishing email threats to prevent future incidents of this nature."[7]

24. Defendant failed to take appropriate or even the most basic steps to protect the PII/PHI of Plaintiff and other class members from being disclosed.

Plaintiff and the Class Have Suffered Injury as a Result of Defendant's Data Mismanagement

[5] https://www.highmark.com/newsroom/press-releases/highmark-notifies-members-about-data-breach/ (last accessed February 21, 2023)
[6] *Id.*
[7] *Id.*

25. As a result of Defendant's failure to implement and follow even the most basic security procedures, Plaintiff's and Class Members' PII/PHI has been and is now in the hands of unauthorized individuals, which may include thieves, unknown criminals, banks, credit companies, and other potentially hostile individuals. Plaintiff and other Class Members now face an increased risk of identity theft, particularly due to the dissemination of their Social Security Number, and will consequentially have to spend, and will continue to spend, significant time and money to protect themselves due to Defendant's Data Breach.

26. Plaintiff and other class members have had their most personal, sensitive and PII/PHI disseminated to the public at large and have experienced and will continue to experience emotional pain and mental anguish and embarrassment.

27. Plaintiff and class members face an increased risk of identity theft, phishing attacks, and related cybercrimes because of the Data Breach. Those impacted are under heightened and prolonged anxiety and fear, as they will be at risk for falling victim for cybercrimes for years to come.

28. PII/PHI is a valuable property right.[8] The value of PII/PHI as a commodity is measurable.[9] "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

[8] *See* Marc van Lieshout, *The Value of Personal Data*, 457 IFIP ADVANCES IN INFORMATION AND COMMUNICATION TECHNOLOGY 26 (May 2015), https://www.researchgate.net/publication/283668023_The_Value_of_Personal_Data ("The value of [personal] information is well understood by marketers who try to collect as much data about personal conducts and preferences as possible...").

[9] *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 (last visited February 21, 2023).

frameworks."[10] American companies are estimated to have spent over $19 billion on acquiring personal data of consumers in 2018.[11] It is so valuable to identity thieves that once PII/PHI has been disclosed, criminals often trade it on the "cyber black-market," or the "dark web," for many years.

29. As a result of its real value and the recent large-scale data breaches, identity thieves and cyber criminals have openly posted credit card numbers, Social Security numbers, 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 aggregated and become more valuable to thieves and more damaging to victims.

30. Personal information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[12] Experian reports that a stolen credit or debit card number can sell for $5 to $110 on the dark web.[13] 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

---

[10] *Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value*, OECD 4 (Apr. 2, 2013), https://www.oecd-ilibrary.org/science-and-technology/exploring-the-economics-of-personal-data_5k486qtxldmq-en.

[11] *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/.

[12] Anita George, *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends (Oct. 16, 2019), https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last visited February 21, 2023).

[13] Brian Stack, *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian (Dec. 6, 2017), https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last visited February 21, 2023).

fetch up to $1,200 to $1,300 each on the black market.[14] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[15] 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.[16]

31. Criminals can use stolen PII/PHI to extort a financial payment by "leveraging details specific to a disease or terminal illness."[17] 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."[18]

32. Consumers place a high value on the privacy of that data. Researchers shed light on how much consumers value their data privacy—and the amount is considerable. Indeed, studies confirm that "when privacy information is made more salient and accessible, some consumers are willing to pay a premium to purchase from privacy protective websites."[19]

---

[14] Adam Greenberg, *Health insurance credentials fetch high prices in the online black market*, SC MAGAZINE (July 16, 2013), https://www.scmagazine.com/news/breach/health-insurance-credentials-fetch-high-prices-in-the-online-black-market (last visited February 21, 2023).

[15] *In the Dark*, VPNOverview.com, 2019, https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last accessed on February 21, 2023).

[16] *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.

[17] *See* n.8, *supra*.

[18] *Id.*

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

33. 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.

34. Indeed, cyberattacks against the healthcare industry have been common for over ten years with the Federal Bureau of Investigation ("FBI") warning as early as 2011 that cybercriminals were "advancing their abilities to attack a system remotely" and "[o]nce a system is compromised, cyber criminals will use their accesses to obtain PII." The FBI further warned that that "the increasing sophistication of cyber criminals will no doubt lead to an escalation in cybercrime."[20]

35. Cyberattacks have become so notorious that the FBI and U.S. Secret Service have issued a warning to potential targets so they are aware of, and prepared for, a potential attack. As one report explained, "[e]ntities like smaller municipalities and hospitals are attractive to ransomware criminals… because they often have lesser IT defenses and a high incentive to regain access to their data quickly.[21]

36. In fact, according to the cybersecurity firm Mimecast, 90% of healthcare organizations experienced cyberattacks in the past year.[22]

---

[20] Gordon M. Snow, *Statement before the House Financial Services Committee, Subcommittee on Financial Institutions and Consumer Credit*, FBI (Sept. 14, 2011), https://archives.fbi.gov/archives/news/testimony/cyber-security-threats-to-the-financial-sector (last visited February 21, 2023).

[21] Ben Kochman, *FBI, Secret Service Warn of Targeted Ransomware*, LAW360 (Nov. 18, 2019), https://www.law360.com/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware (last visited February 21, 2023).

[22] *See* Maria Henriquez, *Iowa City Hospital Suffers PIIshing Attack,* SECURITY MAGAZINE (Nov. 23, 2020), https://www.securitymagazine.com/articles/93988-iowa-city-hospital-suffers-PIIshing-attack (last visited February 21, 2023).

37. Defendant was on notice that the FBI has recently been concerned about data security regarding entities that store certain amounts of PHI, as Defendant does. In August 2014, after a cyberattack on Community Health Systems, Inc., the FBI warned companies within the healthcare industry that hackers were targeting them. The warning stated that "[t]he FBI has observed malicious actors targeting healthcare related systems, perhaps for the purpose of obtaining the Protected Healthcare Information (PHI) and/or Personally Identifiable Information (PII)."[23]

38. Plaintiff and members of the Class, as a whole, must immediately devote time, energy, and money to: 1) closely monitor their medical statements, bills, records, and credit and financial accounts; 2) change login and password information on any sensitive account even more frequently than they already do; 3) more carefully screen and scrutinize phone calls, emails, and other communications to ensure that they are not being targeted in a social engineering or spear phishing attack; and 4) search for suitable identity theft protection and credit monitoring services, and pay to procure them.

39. Once PII is exposed, there is virtually no way to ensure that the exposed information has been fully recovered or contained against future misuse. For this reason, Plaintiff and Class members will need to maintain these heightened measures for years, and possibly their entire lives, as a result of Defendant's conduct. Further, the value of Plaintiff's and Class members' PII has been diminished by its exposure in the Data Breach.

40. As a result of Defendant's failures, Plaintiff and Class Members are at substantial risk of suffering identity theft and fraud or misuse of their PII.

---

[23] Jim Finkle, *FBI Warns Healthcare Firms that they are Targeted by Hackers*, REUTERS (Aug. 2014), https://www.reuters.com/article/us-cybersecurity-healthcare-fbi/fbi-warns-healthcare-firms-they-are-targeted-by-hackers-idUSKBN0GK24U20140820 (last visited February 21, 2023

41. Plaintiff and the Class suffered actual injury from having PII compromised as a result of Defendant's negligent data management and resulting Data Breach including, but not limited to (a) damage to and diminution in the value of their PII/PHI, a form of property that Defendant obtained from Plaintiff; (b) violation of their privacy rights; and (c) present and increased risk arising from the identity theft and fraud.

42. For the reasons mentioned above, Defendant's conduct, which allowed the Data Breach to occur, caused Plaintiff and members of the Class these significant injuries and harm.

43. Plaintiff brings this class action against Defendant for Defendant's failure to properly secure and safeguard PII/PHI and for failing to provide timely, accurate, and adequate notice to Plaintiff and other class members that their PII/PHI had been compromised.

44. Plaintiff, individually and on behalf of all other similarly situated individuals, alleges claims in negligence, negligence per se, breach of implied contract, breach of fiduciary duty, and unjust enrichment.

CLASS ACTION ALLEGATIONS

45. Representative Plaintiff brings this action pursuant to the provisions of Rules 23(a), (b)(2), and (b)(3) of the Federal Rules of Civil Procedure, on behalf of herself and the following classes/subclass(es) (collectively, the "Class"):

Nationwide Class:

"All individuals within the Unites States of America whose PHI/PII and/or financial information was exposed to unauthorized third-parties as a result of the data breach discovered by Defendant on February 6, 2023."

Pennsylvania Subclass:

"All individuals within the Commonwealth of Pennsylvania whose PHI/PII was stored by Defendant and/or was exposed to unauthorized third parties as a result of the data breach discovered by Defendant on February 6, 2023."

46. Excluded from the Classes are the following individuals and/or entities: Defendant's officers and directors, and any entity in which Defendant has a controlling interest; and the affiliates, legal representatives, attorneys, successors, heirs, and assigns of Defendant. Excluded also from the Classes are Members of the judiciary to whom this case is assigned, their families and Members of their staff.

47. Also, in the alternative, Representative Plaintiff requests additional Subclasses as necessary based on the types of PHI/PII that were compromised.

48. Representative Plaintiff reserves the right to amend the above definition or to propose subclasses in subsequent pleadings and motions for class certification.

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

a. Numerosity: A class action is the only available method for the fair and efficient adjudication of this controversy. The Members of the Classes are so numerous that joinder of all of them is impracticable. As noted above, there are at least 300,000 Members.

b. Commonality: Representative Plaintiff and the Class Members share a community of interests in that there are numerous common questions and issues of fact and law which predominate over any questions and issues solely affecting individual members, including but not necessarily limited to:

i. Whether Defendant unlawfully used, maintained, lost, or disclosed Plaintiff's and Class Members' PII/PHI;

ii. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

iii. Whether Defendant's data security systems prior to and during the Data

Breach complied with applicable data security laws and regulations;

iv. Whether Defendant's data security systems prior to and during the Data Breach were consistent with industry standards;

v. Whether Defendant owed a duty to Class Members to safeguard their PII/PHI;

vi. Whether Defendant breached its duty to Class Members to safeguard their PII/PHI;

vii. Whether computer hackers obtained Class Members' PII/PHI in the Data Breach;

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

ix. Whether Defendant's conduct was negligent;

x. Whether Defendant's acts, inactions, and practices complained of herein amount to acts of intrusion upon seclusion under the law;

xi. Whether Defendant's acts breaching an implied contract they formed with Plaintiff and the Class Members;

xii. Whether Defendant violated the Federal Trade Commission Act ("FTC Act");

xiii. Whether Defendant violated the Health Insurance Portability and Accountability Act ("HIPAA");

xiv. Whether Defendant was unjustly enriched to the detriment of Plaintiff and the Class;

xv. Whether Defendant failed to provide notice of the Data Breach in a timely

manner; and

xvi. Whether Plaintiff and Class Members are entitled to damages, civil penalties, punitive damages, and/or injunctive relief.

c. Typicality: Plaintiff's claims are typical of those of other Class Members because Plaintiff's PII/PHI, like that of every other Class Member, was compromised in the Data Breach.

d. Adequacy of Representation: Plaintiff will fairly and adequately represent and protect the interests of the Members of the Class. Plaintiff's Counsel are competent and experienced in litigating class actions, including data privacy litigation of this kind.

e. Fairness, Efficiency and Superiority of Class Action: A class action provides for fair and efficient adjudication of the controversy, and is indeed is superior to other available methods for adjudication. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Defendant. In contrast, the conduct of this action as a class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class Member.

f. Predominance. Defendant has engaged in a common course of conduct toward Plaintiff and Class Members, in that all the Plaintiff's and Class Members' data was stored on the same computer systems and unlawfully accessed in the same way. The common issues arising from Defendant's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

50. This class action is also appropriate for certification because Defendant has acted or refused to act on grounds generally applicable to Class Members, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members and making final injunctive relief appropriate with respect to the Class in its entirety. Defendant's policies and practices challenged herein apply to and affect Class Members

uniformly and Representative Plaintiff's challenge of these policies and practices hinges on Defendant's conduct with respect to the Class in its entirety, not on facts or law applicable only to Representative Plaintiff.

51. Unless a Class-wide injunction is issued, Defendant may continue in its failure to properly secure the PHI/PII and/or financial information of Class Members, and Defendant may continue to act unlawfully as set forth in this Complaint.

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

53. Finally, all members of the proposed Classes are readily ascertainable. Defendant has access to Class Members' names and addresses affected by the Data Breach. At least some Class Members have already been preliminarily identified and sent notice of the Data Breach by Defendant.

CAUSES OF ACTION

COUNT I
NEGLIGENCE

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

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

56. Highmark knew, or should have known, the risks of collecting and storing Plaintiff's and all other Class members' PII/PHI and the importance of maintaining secure systems.

Highmark knew, or should have known, of the vast uptick in data breaches in recent years. Highmark had a duty to protect the PII/PHI of Plaintiff and Class Members.

57. Given the nature of Highmark's business, the sensitivity and value of the PII/PHI it maintains, and the resources at its disposal, Highmark should have identified the vulnerabilities to its systems and prevented the Data Breach from occurring, which Highmark had a duty to prevent.

58. Highmark 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.

59. It was reasonably foreseeable to Highmark that its 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.

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

61. As a result of Highmark's above-described wrongful actions, inaction, and want of ordinary care that directly and proximately caused the Data Breach, Plaintiff and all other Class Members have suffered, and will continue to suffer, economic damages and other injury and actual harm in the form of, *inter alia*: (i) a substantially increased risk of identity theft and medical theft—

risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (ii) improper disclosure of their PII/PHI; (iii) breach of the confidentiality of their PII/PHI; (iv) deprivation of the value of their PII/PHI, for which there is a well-established national and international market; (v) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of medical identity theft they face and will continue to face; and (vii) actual or attempted fraud.

COUNT II
NEGLIGENCE PER SE

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

63. Highmark's duties arise from, in part due to its storage of certain medical information, *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").

64. Highmark'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 Highmark, of failing to employ reasonable measures to protect and secure PII/PHI.

65. Highmark's duties further arise from the Health Insurance Portability and Accountability Act of 1996 (HIPAA), 42 U.S.C. § 1302(d), *et seq.*

66. Highmark is an entity covered under HIPAA, which sets minimum federal standards for privacy and security of PHI.

67. Highmark 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. Highmark'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 Plaintiff and the other Class members.

68. Highmark's violations of HIPAA Privacy and Security Rules and Section 5 of the FTCA constitutes negligence per se.

69. 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.

70. 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.

71. It was reasonably foreseeable to Highmark that its 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.

72. The injury and harm that Plaintiff and the other Class members suffered was the direct and proximate result of Highmark'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) 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) actual or attempted fraud.

COUNT III
BREACH OF FIDUCIARY DUTY

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

74. Plaintiff and Class members either directly or indirectly gave Highmark their PII/PHI in confidence, believing that Highmark – a healthcare and health insurance organization – would protect that information. Plaintiff and Class members would not have provided Highmark with this information had they known it would not be adequately protected. Highmark's acceptance and storage of Plaintiff's and Class members' PII/PHI created a fiduciary relationship between Highmark and Plaintiff and Class Members. In light of this relationship, Highmark must act primarily for the benefit of its clients and health plan participants, which includes safeguarding and protecting Plaintiff's and Class Members' PII/PHI.

75. Highmark 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 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 the PII/PHI of Plaintiff and Class Members it collected.

76. As a direct and proximate result of Highmark's breaches of its fiduciary duties, Plaintiff and Class members have suffered and will suffer injury, including, but not limited to: (i) a substantial increase in the likelihood of identity theft; (ii) the compromise, publication, and theft of their 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 Highmark'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) actual or attempted fraud.

COUNT IV
UNJUST ENRICHMENT

77. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein. This claim is pled in the alternative to the implied contract claim pursuant to Fed. R. Civ. P. 8(d).

78. Plaintiff and Class Members conferred a monetary benefit upon Highmark in the form of monies paid for healthcare services or other services.

79. Highmark accepted or had knowledge of the benefits conferred upon it by Plaintiff and Class Members. Highmark also benefitted from the receipt of Plaintiff's and Class Members' PII/PHI.

80. As a result of Highmark's 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.

81. Highmark should not be permitted to retain the money belonging to Plaintiff and Class Members because Highmark 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.

82. Highmark 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 V
BREACH OF IMPLIED CONTRACT

83. Plaintiff realleges and incorporates by reference all allegations of the preceding factual allegations as though fully set forth herein.

84. Defendant required Plaintiff and Class Members to provide, or authorize the transfer of, their PII/PHI in order for Highmark to provide services. In exchange, Highmark entered into implied contracts with Plaintiff and Class Members in which Highmark agreed to comply with its statutory and common law duties to protect Plaintiff's and Class Members' PII/PHI and to timely notify them in the event of a data breach.

85. Plaintiff and Class Members would not have provided their PII/PHI to Defendant had they known that Defendant would not safeguard their PII/PHI, as promised, or provide timely notice of a data breach.

86. Plaintiff and Class Members fully performed their obligations under their implied contracts with Defendant.

87. Defendant breached the implied contracts by failing to safeguard Plaintiff's and Class Members' PII/PHI and by failing to provide them with timely and accurate notice of the Data Breach.

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

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of the Classes, pray for judgment as follows:

a. For an Order certifying this action as a class action and appointing Plaintiff and her counsel to represent the Class and Subclass;

b. For equitable relief enjoining Highmark from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and Class Members' PII/PHI;

c. For equitable relief compelling Defendant to utilize appropriate methods and policies with respect to consumer data collection, storage, and safety, and to disclose with specificity the type of PII/PHI compromised during the Data Breach;

d. For an order requiring Defendant to pay for credit monitoring services for Plaintiff and the Class of a duration to be determined at trial;

e. For an award of actual damages, compensatory damages, statutory damages, and statutory penalties, in an amount to be determined, as allowable by law;

f. For an award of punitive damages, as allowable by law;

g. For an award of attorneys' fees and costs, and any other expense, including expert witness fees;

h. Pre and post-judgment interest on any amounts awarded; and

i. Such other and further relief as this court may deem just and proper.

JURY TRIAL DEMANDED

Plaintiff Marshall demands a trial by jury on all claims so triable.

Dated: February 21, 2023

Respectfully Submitted By:

By: 

Benjamin F. Johns

SHUB LAW FIRM LLC
Jonathan Shub (PA I.D. #53965)
Benjamin F. Johns (PA I.D. #201373)
Samantha Holbrook (PA I.D. #311829)
134 Kings Hwy E., Fl. 2,
Haddonfield, NJ 08033
T: (856) 772-7200
F: (856) 210-9088
jshub@shublawyers.com
bjohns@shublawyers.com
sholbrook@shublawyers.com

Attorneys for Plaintiff and the Proposed Class

ClassAction.org
