UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF PENNSYLVANIA

ANGELA HOLLANDSWORTH, On Behalf of Herself and All Others Similarly Situated, Plaintiff, v. HIGHMARK HEALTH, Defendant.	**Civil Action No.:** 2:23-cv-376 **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiff Angela Hollandsworth ("Plaintiff"), on behalf of herself and all others similarly situated, alleges as and for her Class Action Complaint, the following against Highmark Health ("Highmark" or "Defendant"), based upon his personal knowledge with respect to herself and her own acts, and upon information and belief, upon her own investigation and the investigation of her counsel, as to all other matters, as follows:

I. INTRODUCTION

1. Highmark describes itself as a health and wellness organization located in Pittsburgh, Pennsylvania that operates insurance plans in Pennsylvania, Delaware, West Virginia, and New York with customers in 50 states and the District of Columbia. Highmark's customers are insured patients who are members of their insurance companies ("Members"). This class action is brought on behalf of citizens of all states in the United States who are the victims of a targeted, intentional cyber-attack at Defendant's computer systems that provided third party criminal hackers to access Defendant's computer systems and exfiltrate Members' data from approximately

December 13, 2022 to December 15, 2022 (the "Class" and "Class Members"), publicly exposing the highly sensitive information and medical records of approximately three hundred thousand class members from Defendant's computer network ("the Data Breach").

2. As a healthcare insurer, Highmark knowingly collected Members' personally identifiable information ("PII"), and protected health information ("PHI") (collectively, "Private Information") in confidence, and has a resulting duty to secure, maintain, protect, and safeguard that Private Information against unauthorized access and disclosure through reasonable and adequate security measures.

3. PHI is considered "the most confidential and valuable type of [PII], irrevocable once breached."[1]

4. As a result of the Data Breach, Plaintiff and Class Members suffered ascertainable losses, including but not limited to, a diminution in the value of their private and confidential information, the loss of the benefit of their contractual bargain with Defendant, out-of-pocket expenses, and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach.

5. Plaintiff's and Class Members' sensitive and private personal information—entrusted to Defendant, its officials, and agents—was compromised, unlawfully accessed, and stolen due to the Data Breach. Information compromised in the Data Breach includes names, social security numbers, health insurance enrollment information such as the insureds' group name, identification number, medical claims or medical treatment information (including procedures and

[1] Junyuan Ke et al, My Data or My Health? Heterogenous Patient Responses to Healthcare Data Breach (February 2, 2022), available at: http://dx.doi.org/10.2139/ssrn.4029103 (last accessed March 7, 2023).

prescription information), financial information, address, phone number and email address, as well as other Private Information and protected health information defined by HIPPA.[2]

6. Plaintiff brings this class action lawsuit on behalf of all those similarly situated to address Defendant's inadequate safeguarding of Class Members' Private Information, for failing to provide timely and adequate notice to Plaintiff and other Class Members of the unauthorized access to their Private Information by an unknown third-party, and for failing to provide timely and adequate notice of precisely what information was accessed and stolen.

7. Defendant breached its duty to Plaintiff and Class Members by maintaining Plaintiff's and the Class Members' Private Information in a negligent and reckless manner.

8. Upon information and belief, the means of the Data Breach and potential for improper disclosure of Plaintiff's and Class Members' Private Information were known and foreseeable risks to Defendant. Thus, Defendant was on notice that failing to take steps necessary to secure the Private Information from those risks left the Private Information in a dangerous and vulnerable condition.

9. Defendant and its employees failed to properly monitor the computer network and systems housing the Private Information.

---

[2] Under the Health Insurance Portability and Accountability Act, 42 U.S.C. § 1320d *et seq.* ("HIPAA"), PHI is considered to be individually identifiable information relating to the past, present, or future health status of an individual that is created, collected, or transmitted, or maintained by a HIPAA-covered entity in relation to the provision of healthcare, payment for healthcare services, or use in healthcare operations. 45 C.F.R. § 160.103. Health information such as diagnoses, treatment information, medical test results, and prescription information are considered protected health information under HIPAA, as are national identification numbers and demographic information such as birth dates, gender, ethnicity, and contact and emergency contact information. *Summary of the HIPAA Privacy Rule*, *available at*: https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html (last accessed March 7, 2023).

10. Had Defendant properly monitored its property, it would have discovered the intrusion sooner or been able to wholly prevent it.

11. Exacerbating an already devastating privacy intrusion, Plaintiff's and Class Members' identities are now at risk because of Defendant's negligent conduct since the Private Information that Defendant collected and stored is now in the hands of data thieves.

12. Armed with the Private Information accessed in the Data Breach, data thieves have data from Highmark to commit a variety of crimes, including credit/debit card fraud, opening new financial accounts in Class Members' names, taking out loans in Class Members' names, using Class Members' names to obtain medical services, using Class Members' health information to target other phishing and hacking intrusions based upon their individual health needs, using Class Members' information to obtain government benefits, filing fraudulent tax returns using Class Members' information, obtaining driver's licenses in Class Members' names but with another person's photograph, and giving false information to police during an arrest.

13. As a direct result of the Data Breach, Plaintiff and Class Members have suffered fraud and identify theft in their financial accounts – including checking accounts connected to debit cards and checks used to pay invoices for services at Highmark – and continue to be exposed to a heightened and imminent risk of fraud and identity theft, potentially for the rest of their lives. Plaintiff and Class Members must now and in the future closely monitor their financial accounts to guard against identity theft.

14. Plaintiff and Class Members already have incurred, and will continue to incur, out-of-pocket costs for purchasing credit monitoring services, credit freezes, credit reports, and other protective measures to deter and detect identity theft.

15. As a direct and proximate result of the Data Breach and subsequent exposure of their Private Information, Plaintiff and Class Members have suffered, and will continue to suffer, damages and economic losses in the form of lost time needed to take appropriate measures to avoid unauthorized and fraudulent charges, putting alerts on their credit files, and dealing with spam messages and e-mails received as a result of the Data Breach. Plaintiff and Class Members have suffered, and will continue to suffer, an invasion of their property interest in their own PII and PHI such that they are entitled to damages from Defendant for unauthorized access to, theft of, and misuse of their PII and PHI. These harms are ongoing, and Plaintiff and Class Members will suffer from future damages associated with the unauthorized use and misuse of their PII and PHI as thieves will continue to use the information to obtain money and credit in their names for several years.

16. Plaintiff seeks to remedy these harms on behalf of all similarly situated individuals whose Private Information was accessed and/or removed from Defendant's network during the Data Breach.

17. Accordingly, Plaintiff brings this action, on behalf of herself and all others similarly situated, against Defendant seeking redress for its unlawful conduct asserting claims for negligence, negligence *per se*, breach of express contract, breach of implied contract, breach of the implied covenant of good faith and fair dealing, negligent misrepresentation, invasion of privacy by intrusion, breach of fiduciary duty, breach of confidence, declaratory judgment, unjust enrichment, and violation of the Pennsylvania Unfair Trade Practices and Consumer Protection Law, 73 Pa. Stat. §§ 201-1 to 201-9.2.

II. PARTIES

18. Plaintiff Angela Hollandsworth ("Plaintiff Hollandsworth") is a resident of Webster County, West Virginia. Plaintiff Hollandsworth was insured by Highmark at all times relevant to the Data Breach. She received letter notice from Highmark that her Private Information was improperly exposed to unauthorized third parties.

19. Defendant Highmark is a Pennsylvania corporation with its principal place of business in Pittsburgh, Pennsylvania. Highmark, through its subsidiary Highmark, Inc., is among the largest health insurers in the United States and the fourth-largest Blue Cross and Blue Shield-affiliated entity. Highmark and its diversified businesses and affiliates operate health insurance plans in Pennsylvania, Delaware, West Virginia, and New York that serve 5.2 million members. Its diversified health businesses serve group customer and individual health needs across the United States through dental insurance, vision care and other related health businesses.

II. JURISDICTION AND VENUE

26. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million, exclusive of interest and costs, there are more than 100 members in the proposed class, and there are thousands of members of the class that are citizens of states different from Defendant.

27. This Court has personal jurisdiction over Defendant because Highmark is headquartered in the Commonwealth of Pennsylvania, its principal place of business is in the Commonwealth of Pennsylvania, and it regularly conducts business in the Commonwealth of Pennsylvania.

28. Venue is proper in this Court pursuant to 28 U.S.C. § 1391 because Defendant resides in this District, a substantial part of the events, acts, and omissions giving rise to Plaintiff's claims occurred in, was directed to, and/or emanated from this District, Highmark is based in this

District, Highmark maintains Members' Private Information in this District, and Defendant has caused harm to Plaintiff and Class Members residing in this District.

III. STATEMENT OF FACTS

A. Highmark's Business.

29. Due to the nature of its services, Highmark must store Members' Private Information and Private Health Information in its system. Highmark accomplishes this by keeping the PII and PHI electronically, as evidenced by this Data Breach.

30. Members demand and are entitled to security to safeguard their Private Information. As a healthcare insurer, Highmark is required to ensure that such private, personal information is not disclosed or disseminated to unauthorized third parties without Members' express, written consent, as further detailed below.

B. The Data Breach.

31. Beginning on or around December 13, 2022 through December 15, 2022, a "threat actor" (an unauthorized cybercriminal who intentionally causes digital harm) allegedly accessed Highmark employee email containing Class Members' Private Information and acquired Plaintiff's and Class Members' PHI and PII. The unauthorized third-party threat actor maintained uninterrupted access to the PHI and PII contained in Highmark employee email, including that of Plaintiff and Class Members, for at least two days. The unauthorized third-party computer hackers allegedly exfiltrated the Private Information of Plaintiff and Class Members from Highmark's computer system and exposed the Private Information for sale to other cybercriminals.

32. After learning of the issue, Highmark commenced an investigation. The investigation further revealed that information accessed and taken by the hackers includes Members' names, medical information, prescription data, information related to their use of medical services, Social Security numbers, financial information and other Private Information that Highmark collected and maintained.

33. Highmark sent a Data Breach Notice ("Notice") informing Members of the data breach beginning in February 2023. Defendant assured Class Members in the Notice that it takes "the security and privacy of all information very seriously" and that Highmark makes "every effort to ensure that confidential information is protected and secure."

34. The Notice recommends that Plaintiff and Class Members regularly review their accounts and periodically obtain their credit reports from one or more of the national credit reporting companies. Defendant advises that Plaintiff and Class Members have the right to put a security freeze, also known as a credit freeze, on their credit files so that no new credit can be opened in their name without the use of a PIN. Likewise, Highmark further advises of placing a fraud alert on their consumer credit file. Plaintiff and Class Members are likewise advised to regularly review the explanation of benefits statement that they receive from their insurer to see if there are any services that they believe they did not receive, to check medical bills, and to request copies of medical records, among others.

35. Given the intentional and criminal nature of the cybersecurity hack, Plaintiff's and Class Members' Private Information is now for sale to criminals on the dark web; meaning unauthorized parties have accessed and viewed Plaintiff's and Class Members' unencrypted, unredacted information, including name, date of birth, billing and insurance information, relevant medical records, prescription data, Social Security numbers, and more.

C. Plaintiff's Experiences Following the Data Breach

Plaintiff Angela Hollandsworth

40. Plaintiff Hollandsworth was an insured medical patient with Highmark at all times relevant to this action.

41. Plaintiff Hollandsworth's PII and PHI was available to Highmark through her status as an insured medical patient.

42. Plaintiff Hollandsworth received a letter informing her of the Data Breach.

43. Thereafter, Plaintiff Hollandsworth spent time taking action to mitigate the impact of the Data Breach after she received the Highmark Notice, which included diligently checking her accounts and her financial accounts. This is time Plaintiff Hollandsworth otherwise would have spent performing other activities or leisurely events for the enjoyment of life.

44. As a result of the Data Breach, Plaintiff has suffered emotional distress as a result of the release of her protected health information which she expected Highmark to protect from disclosure, including anxiety, concern, and unease about unauthorized parties viewing and potentially using her personal and medical information.

45. Plaintiff Hollandsworth suffered actual injury from having her Private Information exposed as a result of the Data Breach including, but not limited to (a) paying monies to Highmark for its goods and services which she would not have paid had Highmark disclosed that it lacked data security practices adequate to safeguard patients' Private Information from theft; (b) damages to and diminution in the value of her Private Information—a form of intangible property that Plaintiff entrusted to Highmark as a condition for healthcare services; (c) loss of her privacy; and (d) imminent and impending injury arising from the increased risk of fraud and identity theft.

46. As a result of the Data Breach, Plaintiff Hollandsworth will continue to be at heightened risk for financial fraud, medical fraud and identity theft, and the attendant damages, for years to come.

D. Highmark Privacy Policies.

101. In Highmark's Privacy Practice statement on its website at www.highmark/privacy.com, it states that "all the information that they collect from you – our users – or that you provide to us is secured and maintained in accordance with a variety of state and federal laws and regulations, as well as our robust corporate standards." In addition, Highmark further states that" it takes the issue of online privacy seriously…."

102. By failing to protect Plaintiff's and Class Members' Private Information, and by allowing the Data Breach to occur, Highmark broke these promises to Plaintiff and Class

Members.

E. The Healthcare Sector is Particularly Susceptible to Cyberattacks.

103. Defendant was specifically on notice that the FBI has been concerned about data security in the healthcare industry. 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)."[3]

104. The number of U.S. data breaches surpassed 1,000 in 2016, a record high and a forty percent increase in the number of data breaches from the previous year.[4] In 2017, a new record high of 1,579 breaches were reported representing a 44.7 percent increase.[5] That trend continues.

105. The healthcare sector reported the second largest number of breaches among all measured sectors in 2018, with the highest rate of exposure per breach.[6] Indeed, when compromised, healthcare related data is among the most sensitive and personally consequential. A report focusing on healthcare breaches found that the "average total cost to resolve an identity theft-related incident . . . came to about $20,000," and that the victims were often forced to pay

---

[3] 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 March 7, 2023).

[4] Identity Theft Resource Center, *Data Breaches Increase 40 Percent in 2016, Finds New Report From Identity Theft Resource Center and CyberScout* (Jan. 19, 2017), *available at:* https://www.idtheftcenter.org/surveys-studys (last accessed March 7.2023).

[5] Identity Theft Resource Center, *2017 Annual Data Breach Year-End Review, available at:* https://www.idtheftcenter.org/2017-data-breaches/ (last accessed March 7, 2023).

[6] Identity Theft Resource Center, *2018 End -of-Year Data Breach Report, available at*: https://www.idtheftcenter.org/2018-data-breaches/ (last accessed March 7, 2023).

out-of-pocket costs for healthcare they did not receive in order to restore coverage.[7] Almost 50 percent of the victims lost their healthcare coverage as a result of the incident, while nearly 30 percent said their insurance premiums went up after the event. Forty percent of the customers were never able to resolve their identity theft at all. Data breaches and identity theft have a crippling effect on individuals and detrimentally impact the economy as a whole.[8]

106. Healthcare related data breaches have continued to rapidly increase. According to the 2019 HIMSS Cybersecurity Survey, 82 percent of participating hospital information security leaders reported having a significant security incident in the last 12 months, with a majority of these known incidents being caused by "bad actors" such as cybercriminals.[9] "Hospitals have emerged as a primary target because they sit on a gold mine of sensitive personally identifiable information for thousands of patients at any given time. From social security and insurance policies, to next of kin and credit cards, no other organization, including credit bureaus, have so much monetizable information stored in their data centers."[10]

107. As a healthcare insurer, Highmark knew, or should have known, the importance of safeguarding its Members' PII and PHI entrusted to it and of the foreseeable consequences if its data security systems were breached. This includes the significant costs that would be imposed on Highmark's Members as a result of a breach. Highmark failed, however, to take adequate cybersecurity measures to prevent the Data Breach from occurring.

---

[7] Elinor Mills, *Study: Medical identity theft is costly for victims*, CNET (March 3, 2010), *available at:* https://www.cnet.com/news/study-medical-identity-theft-is-costly-for-victims/ (last accessed March 7, 2023).

[8] *Id.*

[9] *2019 HIMSS Cybersecurity Survey, available at*: https://www.himss.org/2019-himss-cybersecurity-survey (last accessed March 7, 2023).

[10] Inside Digital Health, *How to Safeguard Hospital Data from Email Spoofing Attacks*, April 4, 2019, *available at*: https://www.idigitalhealth.com/news/how-to-safeguard-hospital-data-from-email-spoofing-attacks (last accessed March 7, 2023).

F. Highmark Acquires, Collects and Stores Its Members' Private Information.

108. Highmark acquires, collects, and stores a massive amount of its Members' PHI and PII.

109. As a condition of engaging in health insurance services, Highmark requires that these Members entrust it with their highly confidential Private Information.

110. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' Private Information, Highmark assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiff's and Class Members' Private Information from disclosure.

111. Plaintiff and Class Members have taken reasonable steps to maintain the confidentiality of their Private Information, and, as current and former Members, they relied on Highmark to keep this information confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

G. The Value of Private Information and the Effects of Unauthorized Disclosure.

112. At all relevant times, Defendant was aware that the Private Information it collects from Plaintiff and Class Members is highly sensitive and of significant value to those who would use it for wrongful purposes.

113. Private Information is a valuable commodity to identity thieves. As the FTC recognizes, identity thieves can use this information to commit an array of crimes including identify theft, and medical and financial fraud.[11] Indeed, a robust "cyber black market" exists in which criminals openly post stolen PII and PHI on multiple underground Internet websites, commonly referred to as the dark web.

[11] Federal Trade Commission, *Warning Signs of Identity Theft, available at:* https://www.consumer.ftc.gov/articles/0271-warning-signs-identity-theft (last accessed March 7, 2023).

114. While credit card information and associated PII can sell for as little as $1-$2 on the black market, PHI can sell for as much as $363 according to the Infosec Institute.[12]

115. PHI is particularly valuable because criminals can use it to target victims with frauds and scams that take advantage of the victim's medical conditions or victim settlements. It can be used to create fake insurance claims, allowing for the purchase and resale of medical equipment, or gain access to prescriptions for illegal use or resale.

116. Medical identify theft can result in inaccuracies in medical records and costly false claims. It can also have life-threatening consequences. If a victim's health information is mixed with other records, it can lead to misdiagnosis or mistreatment. "Medical identity theft is a growing and dangerous crime that leaves its victims with little to no recourse for recovery," reported Pam Dixon, executive director of World Privacy Forum. "Victims often experience financial repercussions and worse yet, they frequently discover erroneous information has been added to their personal medical files due to the thief's activities."[13]

117. Similarly, the FBI Cyber Division, in an April 8, 2014 Private Industry Notification, advised:

> Cyber criminals are selling [medical] information on the black market at a rate of $50 for each partial EHR, compared to $1 for a stolen social security number or credit card number. EHR can then be used to file fraudulent insurance claims, obtain prescription medication, and advance identity theft. EHR theft is also more difficult to detect, taking almost twice as long as normal identity theft.

118. The ramifications of Highmark's failure to keep its Members' Private Information secure are long lasting and severe. Once Private Information is stolen, fraudulent use of that

---

[12] Center for Internet Security, *Data Breaches: In the Healthcare Sector, available at:* https://www.cisecurity.org/blog/data-breaches-in-the-healthcare-sector/ (last accessed March 7, 2023).

[13] Michael Ollove, "The Rise of Medical Identity Theft in Healthcare," Kaiser Health News, Feb. 7, 2014, https://khn.org/news/rise-of-indentity-theft/ (last visited March 7, 2023).

information and damage to victims may continue for years. Fraudulent activity might not show up for six to 12 months or even longer.

119. Further, criminals often trade stolen Private Information on the "cyber black-market" for years following a breach. Cybercriminals can post stolen Private Information on the internet, thereby making such information publicly available.

120. Approximately 21% of victims do not realize their identity has been compromised until more than two years after it has happened. [14] This gives thieves ample time to seek multiple treatments under the victim's name. Forty percent of consumers found out they were a victim of medical identity theft only when they received collection letters from creditors for expenses that were incurred in their names.[15]

121. As a healthcare insurer, Highmark knew, or should have known, the importance of safeguarding its Members' Private Information entrusted to it and of the foreseeable consequences if its data security systems were breached. This includes the significant costs that would be imposed on Highmark's Members due to the breach. Highmark failed, however, to take adequate cybersecurity measures to prevent the Data Breach from occurring.

H. Highmark's Conduct Violates HIPAA.

122. HIPAA requires covered entities to protect against reasonably anticipated threats to the security of PHI. Covered entities must implement safeguards to ensure the confidentiality, integrity, and availability of PHI. Safeguards must include physical, technical, and administrative components.[16]

---

[14] *See* Medical ID Theft Checklist, *available at:* https://www.identityforce.com/blog/medical-id-theft-checklist-2 (last accessed March 7, 2023).

[15] Experian, *The Potential Damages and Consequences of Medical Identify Theft and Healthcare Data Breaches ("Potential Damages"), available at:* https://www.experian.com/assets/data-breach/white-papers/consequences-medical-id-theft-ealthcare.pdf (last accessed March 7, 2023).

[16] HIPAA Journal, *What is Considered Protected Health Information Under HIPAA?, available at:* https://www.hipaajournal.com/what-is-considered-protected-health-information-under-hipaa/ (last accessed March 7, 2023).

123. Title II of HIPAA contains what are known as the Administrative Simplification provisions. 42 U.S.C. §§ 1301, *et seq*. These provisions require, among other things, that the Department of Health and Human Services ("HHS") create rules to streamline the standards for handling Private Information like the data Defendant left unguarded. HHS has subsequently promulgated five rules under authority of the Administrative Simplification provisions of HIPAA.

124. The HIPAA Breach Notification Rule, 45 CFR §§ 164.400-414, also required Defendant to provide notice of the breach to each affected individual "without unreasonable delay and ***in no case later than 60 days following discovery of the breach***."[17]

125. Based on information and belief, Defendant's Data Breach resulted from a combination of insufficiencies that demonstrate Defendant failed to comply with safeguards mandated by HIPAA regulations. Highmark's security failures include, but are not limited to, the following:

i. Failing to ensure the confidentiality and integrity of electronic protected health information that Defendant creates, receives, maintains, and transmits in violation of 45 C.F.R. §164.306(a)(1);
ii. Failing to implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights in violation of 45 C.F.R. §164.312(a)(1);
iii. Failing to implement policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 C.F.R. §164.308(a)(1);
iv. Failing to identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity in violation of 45 C.F.R. §164.308(a)(6)(ii);
v. Failing to protect against any reasonably-anticipated threats or hazards to the security or integrity of electronic protected health information in violation of 45 C.F.R. §164.306(a)(2);
vi. Failing to protect against any reasonably anticipated uses or disclosures of electronically protected health information that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 C.F.R. §164.306(a)(3);

[17] Breach Notification Rule, U.S. Dep't of Health & Human Services, https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html (emphasis added) (last visited March 7, 2023).

vii. Failing to ensure compliance with HIPAA security standard rules by their workforce in violation of 45 C.F.R. §164.306(a)(94);

viii. Impermissibly and improperly using and disclosing protected health information that is and remains accessible to unauthorized persons in violation of 45 C.F.R. §164.502, *et seq.*;

ix. Failing to effectively train all members of their workforce (including independent contractors) on the policies and procedures with respect to protected health information as necessary and appropriate for the members of their workforce to carry out their functions and to maintain security of protected health information in violation of 45 C.F.R. §164.530(b) and 45 C.F.R. §164.308(a)(5); and

x. Failing to design, implement, and enforce policies and procedures establishing physical and administrative safeguards to reasonably safeguard protected health information, in compliance with 45 C.F.R. §164.530(c).

I. Highmark Failed to Comply with FTC Guidelines.

129. Highmark was also prohibited by the Federal Trade Commission Act ("FTC Act") (15 U.S.C. §45) from engaging in "unfair or deceptive acts or practices in or affecting commerce." The Federal Trade Commission ("FTC") has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of the FTC Act. *See, e.g., FTC v. Wyndham Worldwide Corp*., 799 F.3d 236 (3d Cir. 2015).

130. The FTC has promulgated numerous guides for businesses that highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[18]

131. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cybersecurity guidelines for businesses.[19] The guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer

[18] Federal Trade Commission, *Start With Security: A Guide for Business*, *available at:* https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last accessed March 7, 2023).

[19] Federal Trade Commission, *Protecting Personal Information: A Guide for Business*, available at: https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last accessed March 7, 2023).

networks; understand their network's vulnerabilities; and implement policies to correct any security problems.

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

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

134. Highmark failed to properly implement basic data security practices. Highmark's failure to employ reasonable and appropriate measures to protect against unauthorized access to Members' Private Information constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

135. Highmark was at all times fully aware of its obligation to protect the Private Information of Members because of its position as a trusted healthcare insurer. Highmark was also aware of the significant repercussions that would result from its failure to do so.

J. Highmark Failed to Comply with Healthcare Industry Standards.

136. HHS's Office for Civil Rights notes:

> While all organizations need to implement policies, procedures, and technical solutions to make it harder for hackers to gain access to their systems and data, this is especially important in the healthcare

> industry. Hackers are actively targeting healthcare organizations, as they store large quantities of highly Private and valuable data.[20]

137. HHS highlights several basic cybersecurity safeguards that can be implemented to improve cyber resilience that require a relatively small financial investment yet can have a major impact on an organization's cybersecurity posture including: (a) the proper encryption of Private Information; (b) educating and training healthcare employees on how to protect Private Information; and (c) correcting the configuration of software and network devices.

138. Private cybersecurity firms have also identified the healthcare sector as being particularly vulnerable to cyber-attacks, both because of the value of the Private Information which they maintain and because as an industry they have been slow to adapt and respond to cybersecurity threats.[21] They too have promulgated similar best practices for bolstering cybersecurity and protecting against the unauthorized disclosure of Private Information.

139. Despite the abundance and availability of information regarding cybersecurity best practices for the healthcare industry, Highmark chose to ignore them. These best practices were known, or should have been known, by Highmark, whose failure to heed and properly implement them directly led to the Data Breach and the unlawful exposure of Class Members' Private Information.

K. Cyber Criminals Have and Will Continue to Use Plaintiff's and Class Members' Private Information for Nefarious Purposes

140. Plaintiff's and Class Members' highly sensitive Private Information is of great value to hackers and cybercriminals, and the data stolen in the Data Breach can be used in a variety

---

[20] HIPAA Journal, Cybersecurity Best Practices for Healthcare Organizations, https://www.hipaajournal.com/important-cybersecurity-best-practices-for-healthcare-organizations/ (last accessed March 7, 2023).

[21] *See e.g.,* INFOSEC, *10 Best Practices For Healthcare Security, available at:* https://resources.infosecinstitute.com/category/healthcare-information-security/is-best-practices-for-healthcare/10-best-practices-for-healthcare-security/#gref (last accessed March 7, 2023).

of ways for criminals to exploit Plaintiff and Class Members and to profit off their misfortune and stolen information. The cybercriminals' motives for the Data Breach were purely nefarious and malicious in nature: their one goal was to access Highmark's systems in order to obtain valuable Private Information to sell on the dark web.

141. Every year, identity theft causes tens of billions of dollars of losses to victims in the United States.[22] For example, with the Private Information stolen in the Data Breach, including Social Security numbers and financial information, identity thieves can open financial accounts, apply for credit, file fraudulent tax returns, commit crimes, create false driver's licenses and other forms of identification and sell them to other criminals or undocumented immigrants, steal government benefits, give breach victims' names to police during arrests, and many other harmful forms of identity theft.[23] These criminal activities have and will result in devastating financial and personal losses to Plaintiff and Class Members

142. Private Information is such a valuable commodity to identity thieves that once it has been compromised, criminals will use it and trade the information on the cyber black-market for years.

[22] Facts + Statistics: Identity Theft and Cybercrime, Insurance Info. Inst., https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime (discussing Javelin Strategy & Research's report "2018 Identity Fraud: Fraud Enters a New Era of Complexity") (last accessed on March 7, 2023).

[23] *See, e.g.*, Christine DiGangi, 5 Ways an Identity Thief Can Use Your Social Security Number, Nov. 2, 2017, https://blog.credit.com/2017/11/5-things-anidentity-thief-can-do-with-your socialsecurity-number-108597/ (last accessed March 7, 2023).

143. These risks are both certainly impending and substantial. As the FTC has reported, if hackers get access to personally identifiable information, they will use it.[24]

144. Hackers may not use the information right away. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

> [I]n some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[25]

145. For instance, with a stolen Social Security number, which is part of the PII compromised in the Data Breach, someone can open financial accounts, get medical care, file fraudulent tax returns, commit crimes, and steal benefits.[26]

146. If cyber criminals manage to access financial information, health insurance information, and other personally sensitive data—as they did here—there is no limit to the amount of fraud to which Defendant may expose the Plaintiff and Class Members.

L. Plaintiff and Class Members Suffered Damages.

147. The ramifications of Highmark's failure to keep Members' Private Information secure are long lasting and severe. Once Private Information is stolen, fraudulent use of that

---

[24] Ari Lazarus, How fast will identity thieves use stolen info?, FED. TRADE COMM'N (May 24, 2017), https://www.consumer.ftc.gov/blog/2017/05/how-fast-willidentity-thieves-use-stolen-info (last accessed March 7, 2023).

[25] Stolen Laptops Lead to Important HIPAA Settlements, U.S. Dep't of Health and Human Services (Apr. 22, 2014), available at https://wayback.archiveit.org/3926/20170127085330/https://www.hhs.gov/about/news/2014/04/22/stolenlaptops-lead-to-important-hipaa-settlements.html (last accessed March 7, 2023).

[26] *See, e.g.*, Christine DiGangi, 5 Ways an Identity Thief Can Use Your Social Security Number, Nov. 2, 2017, https://blog.credit.com/2017/11/5-things-anidentity-thief-can-do-with-your-socialsecurity-number-108597/ (last accessed March 7, 2023).

information and damage to victims may continue for years. Consumer victims of data breaches are more likely to become victims of identity fraud.[27]

148. In addition to their obligations under state laws and regulations, Defendant owed a common law duty to Plaintiff and Class Members to protect Private Information entrusted to it, including to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the Private Information in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized parties.

149. Defendant further owed and breached its duty to Plaintiff and Class Members to implement processes and specifications that would detect a breach of its security systems in a timely manner and to timely act upon warnings and alerts, including those generated by its own security systems.

150. As a direct result of Defendant's intentional, willful, reckless, and negligent conduct which resulted in the Data Breach, unauthorized parties were able to access, acquire, view, publicize, and/or otherwise cause the identity theft and misuse to Plaintiff's and Class Members' Private Information as detailed above, and Plaintiff is now at a heightened and increased risk of identity theft and fraud.

151. The risks associated with identity theft are serious. While some identity theft victims can resolve their problems quickly, others spend hundreds of dollars and many days repairing damage to their good name and credit record. Some consumers victimized by identity theft may lose out on job opportunities, or be denied loans for education, housing or cars because of negative information on their credit reports. In rare cases, they may even be arrested for crimes they did not commit.

[27] *2014 LexisNexis True Cost of Fraud Study, available at:* https://www.lexisnexis.com/risk/downloads/assets/true-cost-fraud-2014.pdf (last accessed March 7, 2023).

152. Other risks of identity theft include loans opened in the name of the victim, medical services billed in their name, utility bills opened in their name, tax return fraud, and credit card fraud.

153. Plaintiff and Class Members did not receive the full benefit of the bargain, and instead received healthcare insurance and other services that were of a diminished value to that described in their agreements with Highmark and they were damaged in an amount at least equal to the difference in the value of the healthcare insurance with data security protection they paid for and the healthcare insurance they received.

154. As a result of the Data Breach, Plaintiff's and Class Members' Private Information has diminished in value.

155. The Private Information belonging to Plaintiff and Class Members is private, private in nature, and was left inadequately protected by Defendant who did not obtain Plaintiff's or Class Members' consent to disclose such Private Information to any other person as required by applicable law and industry standards.

156. The Data Breach was a direct and proximate result of Defendant's failure to: (a) properly safeguard and protect Plaintiff's and Class Members' Private Information from unauthorized access, use, and disclosure, as required by various state and federal regulations, industry practices, and common law; (b) establish and implement appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of Plaintiff's and Class Members' Private Information; and (c) protect against reasonably foreseeable threats to the security or integrity of such information.

157. Defendant had the resources necessary to prevent the Data Breach, but neglected to adequately implement data security measures, despite its obligation to protect Members' data.

158. Had Defendant remedied the deficiencies in its data security systems and adopted security measures recommended by experts in the field, it would have prevented the intrusions into its systems and, ultimately, the theft of Plaintiff's and Class Members' Private Information.

159. As a direct and proximate result of Defendant's wrongful actions and inactions, Plaintiff and Class Members have been placed at an imminent, immediate, and continuing increased risk of harm from identity theft and fraud, requiring them to take the time which they otherwise would have dedicated to other life demands such as work and family in an effort to mitigate the actual and potential impact of the Data Breach on their lives.

160. The U.S. Department of Justice's Bureau of Justice Statistics found that "among victims who had personal information used for fraudulent purposes, twenty-nine percent spent a month or more resolving problems" and that "resolving the problems caused by identity theft [could] take more than a year for some victims."[28]

161. Defendant's failure to adequately protect Plaintiff's and Class Members' Private Information has resulted in Plaintiff and Class Members having to undertake these tasks, which require extensive amounts of time, calls, and, for many of the credit and fraud protection services, payment of money – while Defendant sits by and does nothing to assist those affected by the incident. Instead, as Highmark's Data Breach Notice indicates, it is putting the burden on Plaintiff and Class Members to discover possible fraudulent activity and identity theft.

162. As a result of Defendant's failures to prevent the Data Breach, Plaintiff and Class Members have suffered, will suffer, and are at increased risk of suffering:

i. The compromise, publication, theft and/or unauthorized use of their Private Information;

ii. Out-of-pocket costs associated with the prevention, detection, recovery and remediation from identity theft or fraud;

iii. Lost opportunity costs and lost wages associated with efforts expended and the loss of productivity from addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent

[28] U.S. Department of Justice, Office of Justice Programs Bureau of Justice Statistics, *Victims of Identity Theft, 2012*, December 2013, *available at*: https://www.bjs.gov/content/pub/pdf/vit12.pdf (last accessed March 7, 2023).

researching how to prevent, detect, contest and recover from identity theft and fraud;

iv. The continued risk to their Private Information, which remains in the possession of Defendant and is subject to further breaches so long as Defendant fails to undertake appropriate measures to protect the Private Information in its possession;

v. Current and future costs in terms of time, effort and money that will be expended to prevent, detect, contest, remediate and repair the impact of the Data Breach for the remainder of the lives of Plaintiff and Class Members; and

vi. Anxiety and distress resulting from fear of misuse of their medical information.

165. In addition to a remedy for the economic harm, Plaintiff and Class Members maintain an undeniable interest in ensuring that their Private Information is secure, remains secure, and is not subject to further misappropriation and theft.

IV. CLASS ALLEGATIONS

170. Plaintiff brings this class action on behalf of herself and on behalf of all others similarly situated pursuant to Rule 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure.

171. The Nationwide Class that Plaintiff seeks to represent is defined as follows:

> **Nationwide Class: All individuals whose Private Information was compromised in the data breach of Highmark's systems from approximately December 13, 2022 to December 15, 2022.**

172. In the alternative to the Nationwide Class, Plaintiff seeks certification of the following state Sub-Class:

> **Pennsylvania Sub-Class: All citizens of the Commonwealth of Pennsylvania whose Private Information was compromised in the data breach of Highmark's systems from approximately December13, 2022 to December 15, 2022.**

173. The Nationwide Class and Pennsylvania Sub-Class are together referred to as the "Classes." Also excluded from the Classes are the following individuals and/or entities: Defendant

and Defendant's parents, subsidiaries, affiliates, officers, and directors, current or former employees, and any entity in which Defendant has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; any and all federal, state or local governments, including but not limited to their departments, agencies, divisions, bureaus, boards, sections, groups, counsels and/or subdivisions; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

174. Plaintiff reserves the right to modify or amend the definition of the proposed Classes before the Court determines whether certification is appropriate.

175. Numerosity, Fed R. Civ. P. 23(a)(1): The Classes are so numerous that joinder of all members is impracticable. Defendant has identified more than 300,000 patients whose Private Information may have been improperly accessed in the Data Breach whose Private Information was compromised, and the Classes are apparently identifiable within Defendant's records.

176. Commonality, Fed. R. Civ. P. 23(a)(2) and (b)(3): Questions of law and fact common to the Classes exist and predominate over any questions affecting only individual Class Members. These include:

i. Whether and when Defendant actually learned of the Data Breach and whether its response was adequate;

ii. Whether Defendant owed a duty to the Classes to exercise due care in collecting, storing, safeguarding and/or obtaining their Private Information;

iii. Whether Defendant breached that duty;

iv. Whether Defendant implemented and maintained reasonable security procedures and practices appropriate to the nature of storing Plaintiff's and Class Members' Private Information;

v. Whether Defendant acted negligently in connection with the monitoring and/or protecting of Plaintiff's and Class Members' PII/PHI;

vi. Whether Defendant knew or should have known that it did not employ reasonable measures to keep Plaintiff's and Class Members' PII/PHI secure and prevent loss or misuse of that Private Information;

vii. Whether Defendant adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

viii. Whether Defendant caused Plaintiff's and Class Members' damages;

ix. Whether Defendant violated the law by failing to promptly notify Members of the Classes that their Private Information had been compromised;

x. Whether Plaintiff and the other Class Members are entitled to actual damages, credit monitoring, and other monetary relief; and

xi. Whether Defendant violated common law and statutory claims alleged herein.

177. Typicality, Fed. R. Civ. P. 23(a)(3): Plaintiff's claims are typical of those of other Class Members, because all had their Private Information compromised as a result of the Data Breach, due to Defendant's misfeasance.

178. Policies Generally Applicable to the Class: This class action is also appropriate for certification because Defendant has acted or refused to act on grounds generally applicable to the Classes, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Classes and making final injunctive relief appropriate with respect to the Class as a whole. Defendant's policies challenged herein apply to and affect the Classes uniformly and Plaintiff's challenge of these policies hinges on Defendant's conduct with respect to the Classes as a whole, not on facts or law applicable only to Plaintiff.

179. Adequacy, Fed. R. Civ. P. 23(a)(4): Plaintiff will fairly and adequately represent and protect the interests of the Class Members in that they have no disabling conflicts of interest that would be antagonistic to those of the other Members of the Classes. Plaintiff seeks no relief that is antagonistic or adverse to the Members of the Classes and the infringement of the rights and the damages he has suffered are typical of other Class Members. Plaintiff has retained counsel experienced in complex consumer class action litigation, and Plaintiff intends to prosecute this action vigorously.

180. Superiority and Manageability, Fed. R. Civ. P. 23(b)(3): The class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action

treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of Class members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain Class Members, who could not individually afford to litigate a complex claim against large corporations, like Defendant. Further, even for those Class Members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

181. The nature of this action and the nature of laws available to Plaintiff and the Classes make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiff and the Classes for the wrongs alleged because Defendant would necessarily gain an unconscionable advantage since Defendant would be able to exploit and overwhelm the limited resources of each individual Member of the Classes with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiff was exposed is representative of that experienced by the Classes and will establish the right of each Class Member to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

182. The litigation of the claims brought herein is manageable. Defendant's uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of the Members of the Classes demonstrates that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

183. Adequate notice can be given to Members of the Classes directly using information maintained in Defendant's records.

184. Unless a Class-wide injunction is issued, Plaintiff and Class Members remain at risk that Defendant will continue to fail to properly secure the Private Information of Plaintiffs

and the Classes resulting in another data breach, continue to refuse to provide proper notification to Class Members regarding the Data Breach, and continue to act unlawfully as set forth in this Complaint.

185. 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 Classes as a whole is appropriate under Rule 23(b)(2) of the Federal Rules of Civil Procedure.

186. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to the following:

i. Whether Defendant owed a legal duty to Plaintiff and the Classes to exercise due care in collecting, storing, using, and safeguarding their Private Information;

ii. Whether Defendant breached a legal duty to Plaintiff and Class Members to exercise due care in collecting, storing, using, and safeguarding their Private Information;

iii. Whether Defendant failed to comply with its own policies and applicable laws, regulations, and industry standards relating to data security;

iv. 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; and

v. Whether Class Members are entitled to actual damages, additional credit monitoring or other injunctive relief, and/or punitive damages as a result of Defendant's wrongful conduct.

COUNT I
NEGLIGENCE
(On Behalf of Plaintiff and the Nationwide Class)

187. Plaintiff repeats and realleges all allegations set forth in paragraphs 1-186 above as if they were fully set forth herein.

188. Defendant required Plaintiff and Class Members to submit PII and PHI in order to obtain insurance coverage and/or to receive health care services.

189. Defendant knew, or should have known, of the risks inherent in collecting and storing the PII and PHI of Plaintiff and Class Members.

190. As described above, Defendant owed duties of care to Plaintiff and Class Members whose PII and PHI had been entrusted with Highmark.

191. Defendant breached its duties to Plaintiff and Class Members by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' PII and PHI.

192. Defendant acted with wanton disregard for the security of Plaintiff's and Class Members' PII and PHI. Defendant knew or should have known that Highmark had inadequate computer systems and data security practices to safeguard such information, and Defendant knew or should have known that hackers were attempting to access the PII and PHI in health care databases, such as Highmark.

193. A "special relationship" exists between Defendant and the Plaintiff and Class Members. Highmark entered into a "special relationship" with Plaintiff and Class Members because Highmark collected the PII and PHI of Plaintiff and the Class Members and stored it in the Highmark Database –information that Plaintiff and the Class Members had been required to provide to Highmark.

194. But for Defendant's wrongful and negligent breach of the duties owed to Plaintiff and the Class Members, Plaintiff and the Class Members would not have been injured.

195. The injury and harm suffered by Plaintiff and Class Members was the reasonably foreseeable result of Defendant's breach of its duties. Defendant knew or should have known it was failing to meet its duties, and that Defendant's breach of such duties would cause Plaintiff and Class Members to experience the foreseeable harms associated with the exposure of their PII and PHI.

196. As a direct and proximate result of Defendant' negligent conduct, Plaintiff and Class Members have suffered injury and are entitled to damages in an amount to be proven at trial.

COUNT II
Negligence *Per Se*
(On behalf of Plaintiff and the Nationwide Class)

197. Plaintiff repeats and realleges all allegations set forth in paragraphs 1-186 above as if they were fully set forth herein.

198. Pursuant to the Federal Trade Commission Act (15 U.S.C. §45), Defendant had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' PII and PHI.

199. Pursuant to HIPAA (42 U.S.C. §1302d et. seq.), Defendant had a duty to implement reasonable safeguards to protect Plaintiff's and Class Members' PII and PHI.

200. Defendant breached its duties to Plaintiff and Class Members under the Federal Trade Commission Act (15 U.S.C. § 45) and HIPAA (42 U.S.C. § 1302d et. seq.), by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' PII and PHI.

201. Defendant's failure to comply with applicable laws and regulations constitutes negligence *per se*.

202. But for Defendant's wrongful and negligent breach of its duties owed to Plaintiff and Class Members, Plaintiff and Class Members would not have been injured.

203. The injury and harm suffered by Plaintiff and Class Members was the reasonably foreseeable result of Defendant's breach of its duties. Defendant knew or should have known that

it was failing to meet its duties, and that Defendant's breach would cause Plaintiff and Class Members to experience the foreseeable harms associated with the exposure of their PII and PHI.

204. As a direct and proximate result of Defendant's negligent conduct, Plaintiff and Class Members have suffered injury and are entitled to damages in an amount to be proven at trial.

COUNT III
Breach of Express Contract
(On behalf of Plaintiff and the Nationwide Class)

205. Plaintiff repeats and realleges all allegations set forth in paragraphs 1-186 above as if they were fully set forth herein.

206. Plaintiff and Class Members entered into written agreements with Defendant as part of the medical services Defendant provided to Plaintiff and Class Members. The agreements involved a mutual exchange of consideration whereby Defendant provided these services in exchange for payment from Class Members, Class Members' insurance carriers, and/or government programs remitting payment on Class Members' behalf.

207. Plaintiff and Class Members and/or their insurance carriers paid Defendant for its services and performed under these agreements.

208. Defendant's failure to protect Plaintiff's and Class Members' PII and PHI constitutes a material breach of the terms of these agreements by Defendant.

209. As a direct and proximate result of Defendant's breaches of express contract, Plaintiff and Class Members have suffered injury and are entitled to damages in an amount to be proven at trial.

COUNT IV
Breach of Implied Contract
(On behalf of Plaintiff and the Nationwide Class)

210. Plaintiff repeats and realleges all allegations set forth in paragraphs 1-186 above as if they were fully set forth herein.

211. Plaintiff and Class Members entered into an implied contract with Highmark when they obtained health care services from Highmark, for which they were required to provide their

PII and PHI. The PII and PHI provided by Plaintiff and Class Members to Highmark was governed by and subject to Highmark's privacy duties and policies.

212. Highmark agreed to safeguard and protect the PII and PHI of Plaintiff and Class Members and to timely and accurately notify them in the event that their PII or PHI was breached or otherwise compromised.

213. Plaintiff and Class Members entered into the implied contracts with the reasonable expectation that Defendant's data security practices and policies were reasonable and consistent with industry standards. Plaintiff and Class Members believed that Highmark would use part of the monies paid to Highmark under the implied contracts to fund adequate and reasonable data security practices.

214. Plaintiff and Class Members would not have obtained health care services from Highmark or provided and entrusted their PII and PHI to Defendant in the absence of the implied contract or implied terms between them and Highmark. The safeguarding of the PII and PHI of Plaintiff and Class Members and prompt and sufficient notification of a breach was critical to realize the intent of the parties.

215. Plaintiff and Class Members fully performed their obligations under the implied contracts with Highmark. Highmark breached its implied contracts with Plaintiff and Class Members to protect their PII and PHI when it (1) failed to have security protocols and measures in place to protect that information; (2) disclosed or allowed disclosure of that information to unauthorized third parties; and (3) failed to provide timely and accurate notice to Plaintiff and Class Members that their PII and PHI was compromised as a result of the Highmark Data Breach.

216. As a direct and proximate result of Highmark's breaches of implied contract, Plaintiff and Class Members sustained actual losses and damages as described in detail above and are also entitled to recover nominal damages.

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

217. Plaintiff repeats and realleges all allegations set forth in paragraphs1-186 above as if they were fully set forth herein.

218. Plaintiff and Class Members entered into valid, binding, and enforceable express or implied contracts with Highmark, as alleged above.

219. These contracts were subject to implied covenants of good faith and fair dealing that all parties would act in good faith and with reasonable efforts to perform their contractual obligations (both explicit and fairly implied) and not to impair the rights of the other parties to receive the rights, benefits, and reasonable expectations under the contracts. These included the implied covenants that Highmark would act fairly and in good faith in carrying out its contractual obligations to take reasonable measures to protect Plaintiff's and Class Members' PII and PHI and to comply with industry standards and federal and state laws and regulations.

220. A "special relationship" exists between Highmark and the Plaintiff and Class Members. Highmark entered into a "special relationship" with Plaintiff and Class Members who sought medical services or treatment at Highmark facilities and, in doing so, entrusted Highmark, pursuant to its requirements, with their PII and PHI.

221. Despite this special relationship with Plaintiff, Highmark did not act in good faith and with fair dealing to protect Plaintiff's and Class Members' PII and PHI.

222. Plaintiff and Class Members performed all conditions, covenants, obligations, and promises owed to Highmark.

223. Highmark's failure to act in good faith in implementing the security measures required by the contracts denied Plaintiff and Class Members the full benefit of their bargain, and instead they received health insurance and related services that were less valuable than what they paid for and less valuable than their reasonable expectations under the contracts. Plaintiff and Class Members were damaged in an amount at least equal to this overpayment.

224. Highmark's failure to act in good faith in implementing the security measures required by the contracts also caused Plaintiff and Class Members to suffer actual damages resulting from the theft of their PII and PHI and they remain at imminent risk of suffering additional damages in the future.

225. Accordingly, Plaintiff and Class Members have been injured as a result of Highmark's breach of the covenant of good faith and fair dealing and are entitled to damages and/or restitution in an amount to be proven at trial.

COUNT VI
Negligent Misrepresentation
(On behalf of Plaintiff and the Nationwide Class)

226. Plaintiff repeats and realleges all allegations set forth in paragraphs 1-186 above as if they were fully set forth herein.

227. Defendant negligently misrepresented material facts, pertaining to the provision of health care services, to Plaintiff and Class Members by representing that it would maintain adequate data privacy and security practices and procedures to safeguard Plaintiff's and Class Members' PII and PHI from unauthorized disclosure, release, data breaches, and theft.

228. Defendant negligently misrepresented material facts, pertaining to the provision of health care services, to Plaintiff and Class Members by representing that it did and would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of Plaintiff's and Class Members' PII and PHI.

229. Because of multiple warnings about the inadequacy of its data privacy and security practices, Defendant either knew or should have known that its representations were not true.

230. In reliance upon these misrepresentations, Plaintiff and Class Members obtained health care services from Defendant.

231. Had Plaintiff and Class Members, as reasonable persons, known of Defendant's inadequate data privacy and security practices, or that Defendant was failing to comply with the requirements of federal and state laws pertaining to the privacy and security of Plaintiff's and Class

Members' PII and PHI, they would not have purchased health services from Defendant, and would not have entrusted their PII and PHI to Defendant.

232. As direct and proximate consequence of Defendant's negligent misrepresentations, Plaintiff and Class Members have suffered the injuries alleged above.

COUNT VII
Invasion of Privacy by Intrusion
(On behalf of Plaintiff and the Nationwide Class)

233. Plaintiff repeats and realleges all allegations set forth in paragraphs 1-186 above as if they were fully set forth herein.

234. Plaintiff and Class Members had a reasonable expectation that Defendant would maintain the privacy of the PII and PHI collected and maintained by Highmark.

235. Defendant represented to Plaintiff and Class Members that it would not disclose their PII and PHI except in a handful of clearly defined and disclosed circumstances.

236. Despite representations to the contrary, Defendant failed to protect and safeguard the PII and PHI entrusted to Highmark by Plaintiff and Class Members and in so doing intruded on the private and personal affairs of Plaintiff and Class Members in a manner highly offensive to a reasonable person; invaded the privacy of Plaintiff and Class Members by disclosing, without authorization, the PHI and PII of Plaintiff and Class Members, inconsistent with both the purpose of the collection of the PII and PHI and inconsistent with the uses of said PII and PHI previously disclosed to Plaintiff and Class Members; failed to provide sufficient security to protect the PII and PHI of Plaintiff and Class Members from unauthorized access; enabled, by failing to protect it sufficiently, the disclosure of PII and PHI without the consent of Plaintiff or Class Members.

237. Highmark knew, or acted with reckless disregard in not knowing, that the PII and PHI collected from Plaintiff and Class Members was, because of its nature, subject to a significant risk of unauthorized access.

238. Highmark knew, or acted with reckless disregard in not knowing, that a reasonable person would consider its failure to adequately protect and secure their PII and PHI to be highly offensive.

239. Highmark's disclosure of Plaintiff's and Class Members' PII and PHI without their consent constituted a violation of the privacy of Plaintiff and Class Members.

240. Highmark's failure to provide sufficient security to protect the PII and PHI of Plaintiff and Class Members, leading to unauthorized access to that data by unauthorized parties constituted the unlawful publication of that PII and PHI by Highmark.

241. The PII and PHI disclosed in the Highmark Data Breach was not generally known to the public and is not a matter of legitimate public concern.

242. Plaintiff and Class Members had a reasonable expectation in the privacy of the PII and PHI that they provided to Highmark. That reasonable expectation was thwarted by Defendant's actions and inactions and Defendant's conduct constituted an invasion of Plaintiff's and Class Members' privacy.

243. As a direct and proximate result of Defendant's negligent conduct, Plaintiff and Class Members have suffered injury and are entitled to damages in an amount to be proven at trial as well as restitution and injunctive relief.

244. As direct and proximate consequence of Defendant's wrongful actions, Plaintiff and Class Members have suffered the injuries alleged above.

COUNT VIII
Breach of Fiduciary Duty
(On behalf of Plaintiff and the Nationwide Class)

245. Plaintiff repeats and realleges all allegations set forth in paragraphs 1-186 above as if they were fully set forth herein.

246. Defendant accepted the special confidence placed in it by Plaintiff and Class Members, even asserting that it "takes the confidentiality, privacy, and security of information in [its] care seriously" and by the promulgation of its Privacy Practice. There was an understanding

between the parties that Defendant would act for the benefit of Plaintiff and Class Members in preserving the confidentiality of the Private Information.

247. Defendant became the guardian of Plaintiff's and the Class Members' Private Information and accepted a fiduciary duty to act primarily for the benefit of its Members, including Plaintiff and the Class Members, including safeguarding Plaintiff's and the Class Members' Private Information.

248. Defendant's fiduciary duty to act for the benefit of Plaintiff and Class Members pertains as well to matters within the scope of its relationship with its Members, in particular, to keep secure the Private Information of those Members.

249. Defendant breached its fiduciary duties to Plaintiff and Class Members by failing to: (a) diligently discover, investigate, or give notice of the Data Breach in a reasonable and practicable period of time; (b) encrypt and otherwise protect the integrity of its computer systems containing Plaintiff's and the Class Members' Private Information; (c) timely notify and/or warn them of the Highmark Data Breach; (d) ensure the confidentiality and integrity of electronic PHI Defendant created, received, maintained, and transmitted, in violation of 45 C.F.R. §164.306(a)(1); (e) 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, in violation of 45 C.F.R. § 164.312(a)(1); (f) implement policies and procedures to prevent, detect, contain, and correct security violations, in violation of 45 C.F.R. § 164.308(a)(1); (g) identify and respond to suspected or known security incidents and to mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity, in violation of 45 C.F.R. § 164.308(a)(6)(ii); (h) protect against any reasonably anticipated threats or hazards to the security or integrity of electronic PHI, in violation of 45 C.F.R. § 164.306(a)(2); (i) protect against any reasonably anticipated uses or disclosures of electronic PHI that are not permitted under the privacy rules regarding individually identifiable health information, in violation of 45 C.F.R. § 164.306(a)(3); (j) ensure compliance with the HIPAA security standard rules by its

workforce, in violation of 45 C.F.R. § 164.306(a)(94); (k) effectively train all members of its workforce (including independent contractors) on the policies and procedures necessary to maintain the security of PHI, in violation of 45 C.F.R. § 164.530(b) and 45 C.F.R. § 164.308(a)(5); (l) design, implement, and enforce policies and procedures establishing physical and administrative safeguards to reasonably safeguard PHI, in violation of 45 C.F.R. § 164.530(c); and (m) by otherwise failing to safeguard Plaintiff's and the Class Members' Private Information.

250. As a direct and proximate result of Defendant's breaches of its fiduciary duties, Plaintiff and Class Members have suffered and/or will suffer injury, including but not limited to: (i) actual identity theft; (ii) the compromise, publication, and/or theft of their Private Information; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their Private Information; (iv) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Highmark Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (v) the continued risk to their Private Information, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information in its continued possession; (vi) future costs in terms of time, effort, and money that will be expended as result of the Highmark Data Breach for the remainder of the lives of Plaintiff and Class Members; and (vii) the diminished value of Defendant's services they received.

251. As a direct and proximate result of Defendant's breaches of its fiduciary duties, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm, and other economic losses.

COUNT IX
Breach of Confidence
(On behalf of Plaintiff and the Nationwide Class)

252. Plaintiff repeats and realleges all allegations set forth in paragraphs 1-186 above as if they were fully set forth herein.

253. At all times during Plaintiff's and the Class Members' interactions with Defendant, Defendant was fully aware of the confidential and sensitive nature of Plaintiff's and the Class Members' PII and PHI that Plaintiffs and the Class Members provided to Defendant.

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

255. Plaintiff and the Class Members receiving treatment from Defendant provided Plaintiff's and the Class Members' PII and PHI to Defendant with the explicit and implicit understandings that Defendant would protect and not permit the PII and PHI to be disseminated to any unauthorized third parties.

256. Plaintiff and the Class Members receiving treatment from Defendant also provided Plaintiff's and the Class Members' PII and PHI to Defendant with the explicit and implicit understanding that Defendant would take precautions to protect that PII and PHI from unauthorized disclosure.

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

258. Due to Defendant's failure to prevent and avoid the Data Breach from occurring, Plaintiff's and the Class Members' PII and PHI was disclosed and misappropriated to unauthorized third parties beyond Plaintiff's and the Class Members' confidence, and without their express permission.

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

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

261. The injury and harm Plaintiff and the Class Members suffered was the reasonably foreseeable result of Defendant's unauthorized disclosure of Plaintiff's and the Class Members' PII and PHI. Defendant knew or should have known its methods of accepting and securing Plaintiff's and the Class Members' PII and PHI was inadequate as it relates to, at the very least, securing servers and other equipment containing Plaintiff's and the Class Members' PII and PHI.

262. As a direct and proximate result of Defendant's breach of its confidence with Plaintiff and the Class Members, Plaintiff and the Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity how their PII and PHI is used; (iii) the compromise, publication, and/or theft of their PII and PHI; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII and PHI; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their PII and PHI, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII and PHI of current and former Members; and (viii) future costs in terms of time, effort, and money that will be expended

to prevent, detect, contest, and repair the impact of the PII and PHI compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and the Class Members.

COUNT X
Declaratory Judgment
(On behalf of Plaintiff and the Nationwide Class)

263. Plaintiff repeats and realleges all allegations set forth in paragraphs 1-186 above as if they were fully set forth herein.

264. Under the Declaratory Judgment Act, 28 U.S.C. §§2201, *et seq.*, this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal and state statutes described in this Complaint.

265. An actual controversy has arisen in the wake of the Data Breach regarding Plaintiff's and Class Members' PII and PHI and whether Highmark is currently maintaining data security measures adequate to protect Plaintiff and Class Members from further data breaches that compromise their PII and PHI. Plaintiff alleges that Highmark's data security measures remain inadequate. Furthermore, Plaintiff and Class Members continue to suffer injury as a result of the compromise of their PII and PHI and remain at imminent risk that further compromises of their PII and/or PHI will occur in the future.

266. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. Highmark owes a legal duty to secure Members' PII and PHI and to timely notify Members of a data breach under the common law, Section 5 of the FTC Act and HIPAA.

b. Highmark breached and continues to breach this legal duty by failing to employ reasonable measures to secure consumers' PII and PHI.

267. This Court also should issue corresponding prospective injunctive relief requiring Highmark to employ adequate security protocols consistent with law and industry standards to protect Members' PII and PHI.

268. If an injunction is not issued, Plaintiff and Class Members will suffer irreparable injury, and lack an adequate legal remedy, in the event of another data breach at Highmark. The risk of another such breach is real, immediate, and substantial. If another breach at Highmark occurs, Plaintiff will not have an adequate remedy at law because many of the resulting injuries are not readily quantified, and he will be forced to bring multiple lawsuits to rectify the same conduct.

269. The hardship to Plaintiff and Class Members if an injunction does not issue exceeds the hardship to Highmark if an injunction is issued. Plaintiff will likely be subjected to substantial identity theft and other damage. On the other hand, the cost to Highmark of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Highmark has a pre-existing legal obligation to employ such measures.

270. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach at Highmark, thus eliminating the additional injuries that would result to Plaintiff, Class Members, and consumers whose confidential information would be further compromised.

COUNT XI
Unjust Enrichment
(On behalf of Plaintiff and the Nationwide Class)

271. Plaintiff repeats and realleges all allegations set forth in paragraphs 1-186 above as if they were fully set forth herein.

272. Plaintiff and Class Members conferred a monetary benefit on Defendant in the form of payments made for the purchase of health care services.

273. Defendant appreciated or had knowledge of the benefits conferred upon it by Plaintiff and Class Members.

274. The payments for healthcare insurance services that Plaintiff and Class Members paid (directly or indirectly) to Defendant should have been used by Defendant, in part, to pay for the administrative costs of reasonable data privacy and security practices and procedures.

275. As a result of Defendant's conduct, Plaintiff and Class Members suffered actual damages in an amount equal to the difference in value between the health care services with the reasonable data privacy and security practices and procedures that Plaintiff and Class Members paid for, and the inadequate health care services without reasonable data privacy and security practices and procedures that they received.

276. Under principles of equity and good conscience, Defendant should not be permitted to retain the money belonging to Plaintiff and Class Members because Defendant failed to implement (or adequately implement) the data privacy and security practices and procedures that Plaintiff and Class Members paid for and that were otherwise mandated by HIPAA regulations, federal, state and local laws, and industry standards.

277. Defendant should be compelled to disgorge into a common fund for the benefit of Plaintiff and Class Members all unlawful or inequitable proceeds received by Defendant.

278. A constructive trust should be imposed upon all unlawful or inequitable sums received by Defendant traceable to Plaintiff and Class Members.

COUNT XII
Pennsylvania Unfair Trade Practices and Consumer Protection Law
73 Pa. Stat. §§ 201-1 to 201-9.2 ("UTPCPL")
(On behalf of Plaintiff and the Pennsylvania Sub-Class)

180. Plaintiff re-alleges and incorporates by reference all preceding allegations in paragraphs 1 through 186 as if fully set forth herein.

181. Plaintiff and Defendant are each a "person" as defined at 73 Pa. Stat. § 201-2(2).

182. Plaintiff and Pennsylvania Class Sub-Class Members purchased goods and services in "trade" and "commerce" as defined at 73 Pa. Stat. § 201-2(3).

183. Plaintiff and Pennsylvania Sub-Class Members purchased goods and services primarily for personal, family, and/or household purposes under 73 Pa. Stat. § 201-9.2.

184. Defendant engaged in "unfair methods of competition" or "unfair or deceptive acts or practices" as defined at 73 Pa. Stat. § 201-2(4) by engaging in the following conduct:

a. Representing that its goods and services had characteristics, uses, benefits, and qualities that they did not have – namely that its goods, services, and business practices were accompanied by adequate data security (73 Pa. Stat. § 201-2(4)(v));

b. Representing that its goods and services were of a particular standard or quality when they were of another quality (73 Pa. Stat. § 201-2(4)(vii));

c. Advertising its goods and services with intent not to sell them as advertised (73 Pa. Stat. § 201-2(4)(ix); and

d. "Engaging in any other . . . deceptive conduct which creates a likelihood of confusion or of misunderstanding" (73 Pa. Stat. § 201-2(4)(xxi)).

185. These unfair methods of competition and unfair or deceptive acts or practices are declared unlawful by 73 Pa. Stat. § 201-3.

186. Defendant's unfair or deceptive acts and practices include but are not limited to: failing to implement and maintain reasonable data security measures to protect Plaintiff's and Pennsylvania Sub-Class Members' Private Information; failing to identify foreseeable data security risks and remediate the identified risks; failing to comply with common law duties, statutory duties and industry standards, including FTC guidance regarding data security; misrepresenting in its Privacy Policy that it would protect cardholder data; and omitting and concealing the material fact that it did not have reasonable measures in place to safeguard Plaintiff's and Pennsylvania Sub-Class Members' PHI and PII.

187. Defendant's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendant's data security practices and ability to protect Plaintiff's and Pennsylvania Sub-Class Members' PHI and PII.

188. Defendant intended to mislead consumers and induce them to rely on its misrepresentations and omissions. As set forth herein, Plaintiff did rely on Defendant's misrepresentations and omissions relating to its data privacy and security.

189. Plaintiff and Pennsylvania Class Members acted reasonably in relying on Defendant's misrepresentations and omissions, the truth of which they could not have discovered with reasonable diligence.

190. Had Defendant disclosed to consumers that its data security systems were not secure and, thus, were vulnerable to attack, Plaintiff and Pennsylvania Sub-Class Members would not have given their PHI and PII to Defendant.

191. Defendant acted intentionally, knowingly, and maliciously in violating the Pennsylvania UTPCPL, and recklessly disregarded consumers' rights.

192. Further, Highmark is a business that compiles or maintains computerized records that include personal information covered under 73 Pa. Stat. § 2301, *et seq*.

193. Under § 2302(a) a business that maintains, stores or manages computerized records that include personal information must notify its Pennsylvania customers of any breach of security of the computerized records following discovery, if the personal information was, or is reasonably believed to have been, accessed by an unauthorized person.

194. As a direct and proximate result of Defendant's unfair methods of competition and unfair or deceptive acts or practices, Plaintiff and Pennsylvania Sub-Class Members have suffered

and will continue to suffer damages, injury, ascertainable losses of money or property, and monetary and non-monetary damages as described above.

195. Plaintiff and Pennsylvania Sub-Class Members seek all monetary and non-monetary relief allowed by law, including the following as expressly permitted under 73 Pa. Stat. § 201-9.2:

a. "actual damages or [statutory damages of] one hundred dollars ($100), whichever is greater";

b. treble damages, defied as "three times the actual damages";

c. "reasonable attorney fees" and litigation costs; and

d. "such additional relief as [the Court] deems necessary or proper."

196. Plaintiff and Pennsylvania Sub-Class Members also seek the injunctive relief as set forth above.

PRAYER FOR RELIEF

A. That the Court certify this action as a class action and certify the Class and Sub-Classes as proper and maintainable pursuant to Rule 23 of the Federal Rules of Civil Procedure; declare that Plaintiff is proper Class and Sub-Class representative; and appoint Plaintiff's Counsel as Class and Sub-Class counsel;

B. That the Court grant permanent injunctive relief to prohibit Highmark from engaging in the unlawful acts, omissions, and practices described herein;

C. That the Court award Plaintiff and Members of the Classes and Sub-Classes compensatory, consequential, and general damages in an amount to be determined at trial;

D. That the Court order disgorgement and restitution of all earnings, profits, compensation, and benefits received by Highmark as a result of its unlawful acts, omissions, and practices;

E. That the Court award statutory damages, trebled, and punitive or exemplary damages, to the extent permitted by law;

F. That Plaintiff be granted the declaratory relief sought herein;

G. That the Court award to Plaintiff the costs and disbursements of the action, along with reasonable attorneys' fees, costs, and expenses;

H. That the Court award pre- and post-judgment interest at the maximum legal rate; and

I. That the Court grant all such other relief as it deems just and proper.

Dated: March 7, 2023

Respectfully submitted,

/s/ Alfred G. Yates, Jr.

Alfred G. Yates, Jr. (PA17419)
Gerald L. Rutledge (PA62027)
LAW OFFICE OF
ALFRED G. YATES, JR., P.C.
1575 McFarland Road, Suite 305
Pittsburgh, PA 15216
Telephone: (412) 391-5164
Fax: (412) 471-1033
yateslaw@aol.com

Lori G. Feldman (*pro hac vice* forthcoming)
GEORGE GESTEN MCDONALD, PLLC
200 Park Avenue, Suite 1700
New York, New York 10166
Telephone: (646) 354-6534
lfeldman@4-justice.com

David J. George (*pro hac vice* forthcoming)
Brittany Brown (*pro hac vice* forthcoming)
GEORGE GESTEN MCDONALD, PLLC
9897 Lake Worth Road, Suite 302
Lake Worth, FL 33467
Telephone: (561) 232-6002
dgeorge@4-justice.com
bbrown@4-justice.com

Janine L. Pollack (*pro hac vice* forthcoming)
CALCATERRA POLLACK LLP
1140 Avenue of the Americas, 9th Floor
New York, NY 10036
Telephone: (212) 899-1760
Jpollack@calcaterrapollack.com

John G. Emerson (*pro hac vice* forthcoming)
EMERSON FIRM, PLLC
2500 Wilcrest Drive
Suite 300
Houston, TX 77042-2754
Telephone: (800) 551.8649
jemerson@emersonfirm.com

Counsel for Plaintiff and the Class