UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF PENNSYLVANIA

STEVEN GRAVLEY, SR., individually and on behalf of all others similarly situated, Plaintiff, v. FRESENIUS VASCULAR CARE, INC. d/b/a AZURA VASCULAR CARE, Defendant.	Case No. **COMPLAINT – CLASS ACTION** JURY TRIAL DEMANDED

Plaintiff Steven Gravley, Sr. ("Plaintiff"), individually and on behalf of all others similarly situated, by and through the undersigned attorneys, brings this class action against Defendant Fresenius Vascular Care, Inc. d/b/a Azura Vascular Care ("Azura" or "Defendant") and complains and alleges upon personal knowledge and information and belief as to all other matters.

INTRODUCTION

1. Plaintiff brings this class action against Azura for its failure to secure and safeguard personally identifiable information ("PII") and personal health information ("PHI") (collectively, "Personal Information") for approximately 348,00 patients of or other persons affiliated with Azura.

2. Defendant is a Pennsylvania-based entity that operates and manages 70 outpatient vascular centers and ambulatory surgery centers in 25 states and Puerto

Rico, with a specialty in minimally invasive techniques to treat various vascular conditions.

3. As a condition of receiving healthcare services, Azura's patients and customers are required to provide and entrust Azura with sensitive and private information, including PII and PHI.

4. On November 9, 2023, Azura confirmed that some of its information had been affected by a cybersecurity incident (the "Data Breach"). Azura conducted incident response and investigated with the assistance of a third-party forensic firm, and reports that starting on or before September 27, 2023, cybercriminals accessed certain systems and encrypted certain files. On November 15, 2023, Azura confirmed that these files included patients' Personal Information.

5. According to Azura, the impacted files contained the following patient information: names, mailing addresses, dates of birth, and other demographic and contact information, including emergency contact information, Social Security numbers, insurance policy and guarantor information, diagnosis and treatment information, and other information from medical or billing records.

6. Azura's January 12, 2024 notice on its website provides scant detail about the Data Breach and the steps that Azura is taking to address it. The notice

merely states that Azura is mailing letters to affected patients and offering credit monitoring services.[1]

7. Azura's notice did not disclose how it discovered the encrypted files on its computer systems were impacted, the means and mechanism of the cyberattack, the reason for the two month delay in disclosing the Data Breach, how Azura determined that the PII/PHI had been "accessed" by the unauthorized actor, and, importantly, what specific steps Azura took following the Data Breach to secure its systems and prevent future cyberattacks.

8. The Data Breach was a direct result of Azura's failure to implement adequate and reasonable cybersecurity procedures and protocols necessary to protect patients' Personal Information from the foreseeable threat of a cyberattack.

9. By being entrusted with Plaintiff's and Class Members' Personal Information for its own pecuniary benefit, Azura assumed a duty to Plaintiff and Class Members to implement and maintain reasonable and adequate security measures to secure, protect, and safeguard Plaintiff's and Class Members' Personal Information against unauthorized access and disclosure. Azura also had a duty to adequately safeguard this Personal Information under controlling case law, as well as pursuant to industry standards and duties imposed by statutes, including HIPAA

[1] *Important Notice for Patients of Azura Vascular Care*, available at: https://www.azuravascularcare.com/notice/ (last accessed on Mar. 14, 2024).

regulations and Section 5 of the Federal Trade Commission Act ("FTC Act"). Azura breached those duties by, among other things, failing to implement and maintain reasonable security procedures and practices to protect its patients' from unauthorized access and disclosure.

10. As a result of Azura's inadequate security and breach of its duties and obligations, the Data Breach occurred, and Plaintiff and approximately 348,000 Class Members suffered injury and ascertainable losses in the form of out-of-pocket expenses, loss of value of their time reasonably incurred to remedy or mitigate the effects of the attack, the diminution in value of their personal information from its exposure, and the present and imminent threat of fraud and identity theft. This action seeks to remedy these failings and their consequences.

11. Azura's failure to timely notify the victims of its Data Breach meant that Plaintiff and Class Members were unable to immediately take affirmative measures to prevent or mitigate the resulting harm.

12. Plaintiff's and Class Members' sensitive and confidential Personal Information remain in the possession of Azura. Absent additional safeguards and independent review and oversight, the information remains vulnerable to further cyberattacks and theft.

13. Azura disregarded the rights of Plaintiff and Class Members by, *inter alia*, failing to take adequate and reasonable measures to ensure its data systems

were protected against unauthorized intrusions; failing to disclose that it did not have adequately robust computer systems and security practices to safeguard patient Personal Information; failing to take standard and reasonably available steps to prevent the Data Breach; failing to properly train its staff and employees on proper security measures; and failing to provide Plaintiff and Class Members prompt and adequate notice of the Data Breach.

14. In addition, Azura and its employees failed to properly monitor the computer network and systems that housed the Personal Information. Had Azura properly monitored these electronic systems, it would have discovered the intrusion sooner or prevented it altogether.

15. The security of Plaintiff's and Class Members' identities is now at risk because of Azura's wrongful conduct as the Personal Information that Azura collected and maintained is now in the hands of data thieves. This present risk will continue for the course of their lives.

16. Armed with the Personal Information accessed in the Data Breach, data thieves can commit a wide range of crimes including, for example, opening new financial accounts in Plaintiff's and Class Members' names, taking out loans in their names, using Plaintiff's and Class Members' identities to obtain government benefits, filing fraudulent tax returns using their information, obtaining driver's

licenses in Plaintiff's and Class Members' names, and giving false information to police during an arrest.

17. As a result of the Data Breach, Plaintiff and Class Members have been exposed to a present and imminent risk of fraud and identity theft. Among other measures, Plaintiff and Class Members must now and in the future closely monitor their financial accounts and medical records to guard against identity theft. Further, Plaintiff and Class Members will incur out-of-pocket costs to purchase credit monitoring and identity theft protection and insurance services, credit freezes, credit reports, or other protective measures to deter and detect identity theft.

18. Plaintiff and Class Members will also be forced to expend additional time to review credit reports and monitor their financial accounts and medical records for fraud or identity theft. And because the exposed information includes health information, Social Security numbers, and other immutable personal details, the risk of identity theft and fraud will persist throughout their lives.

19. Plaintiff and Class Members seek to hold Azura responsible for the harms resulting from the massive and preventable disclosure of such sensitive and personal information. Plaintiff seeks to remedy the harms resulting from the Data Breach on behalf of himself and all similarly situated individuals whose Personal Information was accessed and exfiltrated during the Data Breach.

20. Plaintiff, individually and on behalf of all other Class Members, brings claims for negligence, negligence per se, breach of fiduciary duty, breach of implied contract, unjust enrichment, breach of confidence, and for declaratory and injunctive relief. To remedy these violations of law, Plaintiff and Class Members seek actual damages, statutory damages, restitution, and injunctive and declaratory relief (including significant improvements to Azura's data security protocols and employee training practices); reasonable attorneys' fees, costs, and expenses incurred in bringing this action; and all other remedies this Court deems just and proper.

PARTIES

Plaintiff

Plaintiff Steven Gravley, Sr.

21. Plaintiff Steven Gravley, Sr. is a resident and citizen of the Commonwealth of Pennsylvania.

22. Plaintiff is and/or has been a patient at Azura Vascular Care at its location on Bustleton Avenue in Philadelphia, Pennsylvania. Plaintiff provided PII/PHI to Azura in connection with receiving healthcare services from Azura. In requesting and maintaining Plaintiff's Personal Information for its business purposes, Azura expressly and impliedly promised, and undertook a duty, to act reasonably in its handling of Plaintiff's Personal Information. On information and

belief, Azura did not take proper care of Plaintiff's Personal Information, leading to its exposure and exfiltration by cybercriminals as a direct result of its inadequate security measures. Within a few months after the data breach, Plaintiff believes he suffered medical identity theft as he received an unfamiliar medical bill.

23. Once Personal Information is exposed, there is virtually no way to ensure that the exposed information has been fully recovered or contained against future misuse. For this reason, Plaintiff will need to maintain these heightened measures for years.

24. Plaintiff also suffered actual injury from having Personal Information compromised as a result of the Data Breach, including, but not limited to: (a) damage to and diminution in the value of Plaintiff's confidential personal information—a form of property that Plaintiff entrusted to Azura, which was compromised as a result of the Data Breach it failed to prevent and (b) a violation of Plaintiff's privacy rights as a result of Azura's unauthorized disclosure of Personal Information.

25. Plaintiff greatly values privacy, especially while receiving health services. Had Plaintiff known that Azura does not adequately protect PII/PHI, Plaintiff would not have used Azura's services and agreed to provide Azura with PII/PHI.

26. As a result of Azura's failure to adequately safeguard Plaintiff's information, Plaintiff has been injured. Plaintiff is also at a continued risk of harm

because the Personal Information remains in Azura's systems, which have already been shown to be susceptible to compromise and attack and is subject to further attack so long as Azura fails to undertake the necessary and appropriate data security measures to protect the PII and PHI in its possession.

Defendant

27. Defendant Fresenius Vascular Care, Inc. d/b/a Azura Vascular Care is a corporation formed under the laws of the Commonwealth of Pennsylvania with corporate headquarters located at 40 Valley Stream Parkway, Malvern, Pennsylvania 19355. On information and belief, Azura Vascular Care is a "d/b/a" entity for Fresenius Vascular Care, Inc. ("FVC"). It was formed by and is a wholly owned business unit of Fresenius Medical Care Holdings, Inc., a limited partnership organized under the laws of New York corporation and does business as "Fresenius Medical Care North America." On information and belief, FVC has done business as Azura Vascular Care since 2017.[2]

28. According to its website, Azura presently operates 70 clinics in approximately 25 states (and Puerto Rico) throughout the United States, including three locations in the commonwealth of Pennsylvania.

[2] https://www.azuravascularcare.com/in-the-news/fresenius-vascular-care-announces-new-name/ (last accessed Mar. 15, 2024).

JURISDICTION AND VENUE

29. This Court has jurisdiction over this action pursuant to 28 U.S.C. § 1332(d)(2)(A), as modified by the Class Action Fairness Act of 2005, because at least one member of the Class is a citizen of a different state than Defendant, there are more than 100 members of the Class, and the aggregate amount in controversy exceeds $5,000,000 exclusive of interests and costs.

30. This Court has personal jurisdiction over Azura because Azura maintains its principal place of business in Pennsylvania and conducts substantial business in Pennsylvania and in this district through its principal place of business; engaged in the conduct at issue herein from and within this District; and otherwise has substantial contacts with this District and purposely availed itself of the Courts in this District.

31. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(b)(1) and (2) because Azura resides in this district, and this district is where a substantial part of the acts, omissions, and events giving rise to Plaintiff's claims occurred.

FACTUAL ALLEGATIONS

A. Overview of Azura Health

32. Azura is a Pennsylvania-based entity that operates and manages 70 outpatient vascular centers and ambulatory surgery centers in 25 states and Puerto

Rico, with specialty in minimally invasive techniques to treat various vascular conditions.

33. In the regular course of its business, Azura collects and maintains the PII/PHI of patients, former patients, and other affiliated persons, including those to whom it is currently providing or previously provided health-related or other similar or related services.

34. As a regular part of its business, Azura requires patients to provide personal information before it provides them services. That information includes, *inter alia*, names, mailing addresses, dates of birth, and other demographic and contact information, including emergency contact information, Social Security numbers, insurance policy and guarantor information, diagnosis and treatment information, and other information from medical or billing records. Azura stores this information digitally.

35. Azura is required to implement adequate safeguards to prevent unauthorized use or disclosure of Personal Information, including by implementing requirements of the HIPAA Security Rule[3] and to report any unauthorized use or

[3] The HIPAA Security Rule establishes national standards to protect individuals' electronic personal health information that is created, received, used, or maintained by a covered entity. The Security Rule requires appropriate administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of electronic protected health information. *See* 45 C.F.R. Part 160 and Part 164, Subparts A and C.

disclosure of Personal Information, including incidents that constitute breaches of unsecured protected health information as in the case of the Data Breach complained of herein.

36. In its Privacy Statement, Azura affirms that it "value[s] your trust and [is] committed to the responsible management of Personal Information,"[4] and in its HIPAA Notice of Privacy Practices, Azura states "[w]e understand that your health information is important, and we are committed to protecting your privacy."[5]

37. Yet, Azura waited nearly two months after discovering the data breach to disclose that patient PII/PHI had been compromised.

38. Plaintiff and Class Members are, or were, patients of Azura or received health-related or other services from Azura, or otherwise are affiliated or transacted with Azura, and entrusted Azura with their PII/PHI or otherwise had their PII/PHI entrusted to Azura.

B. Azura Is a HIPAA Covered Business Associate

39. Azura is a healthcare provider that provides healthcare services through 70 locations throughout the United States and Puerto Rico, including in Pennsylvania.

[4] Fresenius Medical Care, *Privacy Statement*, https://fmcna.com/privacy-statement/ (last accessed Mar. 14, 2024).
[5] Fresenius Medical Care, *HIPAA Notice of Privacy Practices*, https://fmcna.com/notice-of-privacy-practices/ (last accessed Mar. 14, 2024).

40. In the regular course of its business, Azura collects and maintains the Personal Information of patients, former patients, and other persons.

41. Azura is a HIPAA covered business associate that provides healthcare services to patients. As a regular and necessary part of its business Azura collects and custodies the highly sensitive Patient Information of its patients. Azura is required under federal and state law to maintain the strictest confidentiality of the patient's Personal Information that it requires, receives, and collects, and Azura is further required to maintain sufficient safeguards to protect that Personal Information from being accessed by unauthorized third parties.

42. As a HIPAA covered business entity, Azura is required to implement adequate safeguards to prevent unauthorized use or disclosure of Personal Information, including by implementing requirements of the HIPAA Security Rule[6] and to report any unauthorized use or disclosure of Personal Information, including incidents that constitute breaches of unsecured protected health information as in the case of the Data Breach complained of herein.

43. As a condition of receiving Azura's services, Azura requires that patients, including Plaintiff and Class Members, entrust it with highly sensitive personal information. Due to the nature of Azura's business of providing health services, Azura would be unable to engage in its regular business activities without

[6] *See* note 2, *supra.*

collecting and aggregating Personal Information that it knows and understands to be sensitive and confidential.

44. Azura recognizes its responsibility, as "required by law," "to make sure that your PHI is kept private; . . . Use or share your information only as described in [its HIPAA Notice of Privacy Practices] . . . ; and Notify you if there is a breach of your unsecured PHI."[7]

45. Plaintiff and Class Members are or were patients whose medical records were maintained by, or who received health-related or other services from, Azura and directly or indirectly entrusted Azura with their Personal Information. Plaintiff and Class Members reasonably expected that Azura would safeguard their highly sensitive information and keep their Personal Information confidential.

C. The Data Breach Compromised Plaintiff's and Class Members' PII/PHI

46. On November 9, 2023, Azura confirmed that some of its information had been affected in the Data Breach. It conducted incident response and investigated with the assistance of a third-party forensic firm. Starting on or before September 27, 2023, cybercriminals accessed certain systems and encrypted certain files. On November 15, 2023, Azura confirmed that these files included patient Personal Information, including names, mailing addresses, dates of birth, and other demographic and contact information, including emergency contact information,

[7] *See HIPAA Notice of Privacy Practices*, note 4, *supra*.

Social Security numbers, insurance policy and guarantor information, diagnosis and treatment information, and other information from medical or billing records.

47. Azura did not publicly announce the Data Breach until two months later, on January 12, 2024.[8] The notice confirms "that a third party impermissibly accessed personal information that may have included health related information found in patient medical and billing records," and states that Azura is mailing letters to affected patients and offering credit monitoring services.[9]

48. Azura's disclosures omit pertinent information including how criminals gained access to the encrypted files on its systems, what computer systems were impacted, the means and mechanisms of the cyberattack, how it determined that the Personal Information had been accessed, and of particular importance to Plaintiff and Class Members, what actual steps Azura took following the Data Breach to secure its systems and train its employees to prevent further cyberattacks.

49. Based on Azura's acknowledgment that Personal Information was accessed by an unauthorized party, it is evident that unauthorized criminal actors did in fact access Azura's network and exfiltrate Plaintiff's and Class Members' Personal Information in an attack designed to acquire that sensitive, confidential, and valuable information.

[8] *See Important Notice for Patients of Azura Vascular Care,* note 1, *supra*.
[9] *Id*.

50. The Personal Information contained in the files accessed by cybercriminals appears not to have been encrypted because if properly encrypted, the attackers would have acquired unintelligible data and would not have "accessed" Personal Information.

51. Azura acknowledges that it operates 70 clinics, but did not confirm whether some or all of its locations were impacted by the Data Breach. The Data Breach reportedly impacted the protected health information of 348,000 individuals.[10]

52. As a HIPAA associated business entity that collects, creates, and maintains significant volumes of private information, the targeted attack was a foreseeable risk of which Azura was aware and knew it had a duty to guard against.

53. The targeted attack was expressly designed to gain access to and exfiltrate private and confidential data, including (among other things) the Personal Information of patients, like Plaintiff and Class Members.

54. Due to Azura's inadequate security measures, Plaintiff and Class Members now face a present, immediate, and ongoing risk of fraud and identity theft and must deal with that threat forever.

[10] U.S. Department of Health and Human Services, *Cases Currently Under Investigation,* https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (last accessed Mar. 14, 2024).

55. Azura had obligations created by HIPAA, contract, industry standards, and common law to Plaintiff and Class Members to keep their Personal Information confidential and to protect it from unauthorized access and disclosure.

56. Plaintiff and Class Members entrusted their Personal Information to Azura, or otherwise had that information provided to Azura, with the reasonable expectation and mutual understanding that Azura or anyone who used their Personal Information in conjunction with the healthcare services they received would comply with obligations to keep such information confidential and secure from unauthorized access after it received such information.

57. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' private information, Azura assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiff's and Class Members' Personal Information from unauthorized disclosure.

58. Plaintiff and the Class Members have taken reasonable steps to maintain the confidentiality of their personal information. Plaintiff and Class Members would not have allowed Azura or anyone in Azura's position to receive their PII/PHI had they known that Azura would fail to implement industry standard protections for that sensitive information.

59. As a result of Azura's negligent and wrongful conduct, Plaintiff's and Class Members' highly confidential and sensitive Personal Information was left exposed to cybercriminals.

D. Defendant Was Obligated Under HIPAA to Safeguard the Personal Information

60. Azura is a covered business associate under HIPAA (45 C.F.R. § 160.102) and is required to comply with the HIPAA Privacy Rule and Security Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and E ("Standards for Privacy of Individually Identifiable Health Information"), and Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C.

61. Azura is subject to the rules and regulations for safeguarding electronic forms of medical information pursuant to the Health Information Technology Act ("HITECH").[11] *See* 42 U.S.C. §17921, 45 C.F.R. § 160.103.

62. HIPAA's Privacy Rule or *Standards for Privacy of Individually Identifiable Health Information* establishes national standards for the protection of health information.

[11] HIPAA and HITECH work in tandem to provide guidelines and rules for maintaining protected health information. HITECH references and incorporates HIPAA.

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

64. HIPAA requires "compl[iance] with the applicable standards, implementation specifications, and requirements" of HIPAA "with respect to electronic protected health information." 45 C.F.R. § 164.302.

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

66. HIPAA's Security Rule requires Azura to do the following:

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

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

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

d. Ensure compliance by its workforce.

67. HIPAA also requires Azura to "review and modify the security measures implemented . . . as needed to continue provision of reasonable and appropriate protection of electronic protected health information." 45 C.F.R. § 164.306(e). Additionally, Azura is required under HIPAA to "[i]mplement 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." 45 C.F.R. § 164.312(a)(1).

68. HIPAA and HITECH also obligated Azura to implement policies and procedures to prevent, detect, contain, and correct security violations, and to protect against uses or disclosures of electronic protected health information that are reasonably anticipated but not permitted by the privacy rules. *See* 45 C.F.R. § 164.306(a)(1) and § 164.306(a)(3); *see also* 42 U.S.C. §17902.

69. The HIPAA Breach Notification Rule, 45 C.F.R. §§ 164.400-414, also requires Azura to provide notice of the Data Breach to each affected individual "without unreasonable delay and in no case later than 60 days following discovery of the breach."[12]

70. HIPAA requires a covered entity to have and apply appropriate sanctions against members of its workforce who fail to comply with the privacy

[12] U.S. Department of Health & Human Services, *Breach Notification Rule*, https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html (last accessed on Mar. 14, 2024) (emphasis added).

policies and procedures of the covered entity or the requirements of 45 C.F.R. Part 164, Subparts D or E. *See* 45 C.F.R. § 164.530(e).

71. HIPAA requires a covered entity to mitigate, to the extent practicable, any harmful effect that is known to the covered entity of a use or disclosure of protected health information in violation of its policies and procedures or the requirements of 45 C.F.R. Part 164, Subpart E by the covered entity or its business associate. *See* 45 C.F.R. § 164.530(f).

72. HIPAA also requires the Office of Civil Rights ("OCR"), within the Department of Health and Human Services ("HHS"), to issue annual guidance documents on the provisions in the HIPAA Security Rule. *See* 45 C.F.R. §§ 164.302-164.318. For example, "HHS has developed guidance and tools to assist HIPAA covered entities in identifying and implementing the most cost effective and appropriate administrative, physical, and technical safeguards to protect the confidentiality, integrity, and availability of e-PHI and comply with the risk analysis requirements of the Security Rule." U.S. Department of Health & Human Services, Security Rule Guidance Material.[13] The list of resources includes a link to guidelines set by the National Institute of Standards and Technology (NIST), which OCR says "represent the industry standard for good business practices with respect to standards

[13] U.S. Department of Health & Human Services, *Security Rule Guidance Material*, http://www.hhs.gov/hipaa/for-professionals/security/guidance/index.html (last accessed on Mar. 14, 2024).

for securing e-PHI." U.S. Department of Health & Human Services, Guidance on Risk Analysis.[14]

E. Azura Failed to Follow FTC Guidelines

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

74. The FTC has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices.

75. According to the FTC, the need for data security should be factored into all business decision-making.

76. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cybersecurity guidelines for businesses.

[14] U.S. Department of Health & Human Services, *Guidance on Risk Analysis*, https://www.hhs.gov/hipaa/for-professionals/security/guidance/guidance-risk-analysis/index.html (last accessed on Mar. 14, 2024).

77. The guidelines note that businesses should protect the personal patient information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.

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

79. The FTC further recommends that companies not maintain private information longer than is needed for authorization of a transaction; limit access to sensitive 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.

80. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect patient 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

FTC Act, 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

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

82. Azura's failure to employ reasonable and appropriate measures to protect against unauthorized access to patients' and plan members' private information constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

83. Azura was at all times fully aware of its obligation to protect the private information of the patients and plan members about whom it stored private information. Azura was also aware of the significant repercussions that would result from its failure to do so.

F. Azura Failed to Comply with Industry Standards

84. As described above, experts studying cybersecurity routinely identify healthcare providers and their business associates as being particularly vulnerable to cyberattacks because of the value of the PII and PHI which they collect and maintain.

85. Several best practices have been identified that at a minimum should be implemented by HIPAA covered business entities like Azura, including but not limited to: educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data

unreadable without a key; multi-factor authentication; backup data; and limiting which employees can access sensitive data.

86. Other best cybersecurity practices that are standard in the healthcare industry include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches, and routers; monitoring and protection of physical security systems; protection against any possible communication system; and training staff regarding critical points.

87. Azura failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

88. These foregoing frameworks are existing and applicable industry standards in the healthcare industry, and Azura failed to comply with these accepted standards, thereby opening the door to cybercriminals and causing the Data Breach.

G. Azura Owed Plaintiff and Class Members a Duty to Safeguard Their Personal Information

89. In addition to its obligations under federal and state laws, Azura owed a duty to Plaintiff and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the Personal Information in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. Azura owed a duty to Plaintiff and Class Members to provide reasonable security, including consistency with industry standards and requirements, and to ensure that its computer systems, networks, and protocols adequately protected the Personal Information of Class Members.

90. Azura owed a duty to Plaintiff and Class Members to create and implement reasonable data security practices and procedures to protect the Personal Information in its possession, including adequately training its employees and others who accessed private information within its computer systems on how to adequately protect Private Information.

91. Azura owed a duty to Plaintiff and Class Members to implement processes that would detect a compromise of Personal Information in a timely manner.

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

93. Azura owed a duty to Plaintiff and Class Members to disclose in a timely and accurate manner when and how the Data Breach occurred.

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

H. Azura Knew That Criminals Target PII/PHI

95. Azura's data security obligations were particularly important given the substantial increase in cyberattacks and/or data breaches in the healthcare industry and other industries holding significant amounts of PII and PHI preceding the date of the breach.

96. At all relevant times, Azura knew, or should have known, its patients', Plaintiff's, and all other Class Members' PII/PHI was a target for malicious actors. Despite such knowledge, Azura failed to implement and maintain reasonable and appropriate data privacy and security measures to protect Plaintiff's and Class Members' Personal Information from cyberattacks that Azura should have anticipated and guarded against.

97. The targeted attack was expressly designed to gain access to and exfiltrate private and confidential data, including (among other things) the Personal Information of patients and/or plan members, such as Plaintiff and Class Members.

98. Cybercriminals seek out PHI at a greater rate than other sources of personal information. In a 2022 report, the healthcare compliance company Proetus

found that there were 905 medical data breaches in 2021, leaving over 50 million patient records exposed for 700 of the 2021 incidents. This is an increase from the 758 medical data breaches that Protenus compiled in 2020.[15]

99. The healthcare sector suffered about 337 breaches in the first half of 2022 alone, according to Fortified Health Security's mid-year report released in July. The percentage of healthcare breaches attributed to malicious activity rose more than 5 percentage points in the first six months of 2022 to account for nearly 80 percent of all reported incidents.[16]

100. Further, a 2022 report released by IBM Security states that for 12 consecutive years the healthcare industry has had the highest average cost of a data breach and as of 2022 healthcare data breach costs have hit a new record high.[17]

101. Personal Information is a valuable property right.[18] The value of

---

[15] *2022 Breach Barometer*, Protenus (2022), https://www.protenus.com/breach-barometer-report

[16] Jill McKeon, *Health Sector Suffered 337 Healthcare Data Breaches in First Half of Year*, Cybersecurity News (July 19, 2022), https://healthitsecurity.com/news/health-sector-suffered-337-healthcare-data-breaches-in-first-half-of-year.

[17] *Cost of a Data Breach Report 2022*, IBM Security (July 2022), https://www.ibm.com/downloads/cas/3R8N1DZJ.

[18] *See* Marc van Lieshout, *The Value of Personal Data*, 457 IFIP Advances in Information and Communication Technology (May 2015), https://www.researchgate.net/publication/283668023 ("The value of [personal] information is well understood by marketers who try to collect as much data about personal conducts and preferences as possible...").

Personal Information as a commodity is measurable.[19] "Firms are now able to attain significant market valuations by employing business models predicated on the successful use of personal data within the existing legal and regulatory frameworks."[20] American companies are estimated to have spent over $19 billion on acquiring personal data of consumers in 2018.[21] It is so valuable to identity thieves that once Personal Information has been disclosed, criminals often trade it on the "cyber black-market," or the "dark web," for many years.

102. As a result of its real value and the recent large-scale data breaches, identity thieves and cybercriminals have openly posted credit card numbers, Social Security numbers, Personal Information, and other sensitive information directly on various internet websites, making the information publicly available. This information from various breaches, including the information exposed in the Data Breach, can be aggregated and become more valuable to thieves and more damaging to victims.

---

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

[20] *Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value*, OECD Digital Economy Papers, No. 220, OECD Publishing (Apr. 2, 2013), https://www.oecd-ilibrary.org/science-and-technology/exploring-the-economics-of-personal-data_5k486qtxldmq-en.

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

103. PHI is particularly valuable and has been referred to as a "treasure trove for criminals."[22] A cybercriminal who steals a person's PHI can end up with as many as "seven to 10 personal identifying characteristics of an individual."[23] A study by Experian found that the "average total cost" of medical identity theft is "about $20,000" per incident, and that a majority of victims of medical identity theft were forced to pay out-of-pocket costs for healthcare they did not receive in order to restore coverage.[24]

104. Personal information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[25] Experian reports that a stolen credit or debit card number can sell for $5 to $110 on the dark web.[26] All-inclusive health insurance dossiers containing sensitive health insurance information, names, addresses, telephone numbers, email addresses, Social Security numbers, and bank

---

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

[23] *Id.*

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

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

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

account information, complete with account and routing numbers, can fetch up to $1,200 to $1,300 each on the black market.[27] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[28] According to a report released by the Federal Bureau of Investigation's ("FBI") Cyber Division, criminals can sell healthcare records for 50 times the price of a stolen Social Security or credit card number.[29]

105. Criminals can use stolen Personal Information to extort a financial payment by "leveraging details specific to a disease or terminal illness."[30] Quoting Carbon Black's Chief Cybersecurity Officer, one recent article explained: "Traditional criminals understand the power of coercion and extortion . . . . By having healthcare information—specifically, regarding a sexually transmitted disease or terminal illness—that information can be used to extort or coerce someone to do what you want them to do."[31]

---

[27] Adam Greenberg, *Health insurance credentials fetch high prices in the online black market*, SC Magazine (July 16, 2013), https://www.scmagazine.com/news/breach/health- insurance-credentials-fetch-high-prices-in-the-online-black-market.
[28] *In the Dark*, VPNOverview.com, https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last accessed on Feb. 23, 2024).
[29] *See Health Care Systems and Medical Devices at Risk for Increased Cyber Intrusions for Financial Gain*, FBI Cyber Division (Apr. 8, 2014), https://www.illuminweb.com/wp-content/uploads/ill-mo-uploads/103/2418/health-systems-cyber-intrusions.pdf.
[30] *See* note 21, *supra*.
[31] *Id.*

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

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

108. Indeed, cyberattacks against the healthcare industry have been common for over ten years with the Federal Bureau of Investigation ("FBI") warning as early as 2011 that cybercriminals were "advancing their abilities to attack a system remotely" and "[o]nce a system is compromised, cyber criminals will use their accesses to obtain PII." The FBI further warned that that "the increasing sophistication of cyber criminals will no doubt lead to an escalation in cybercrime."[33]

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

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

109. Cyberattacks have become so notorious that the FBI and U.S. Secret Service have issued a warning to potential targets so they are aware of, and prepared for, a potential attack. As one report explained, "[e]ntities like smaller municipalities and hospitals are attractive to ransomware criminals … because they often have lesser IT defenses and a high incentive to regain access to their data quickly.[34]

110. In fact, according to the cybersecurity firm Mimecast, 90% of healthcare organizations experienced cyberattacks in the past year.[35]

111. Azura was on notice that the FBI has recently 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)."[36]

---

[34] Ben Kochman, *FBI, Secret Service Warn of Targeted Ransomware*, Law360 (Nov. 18, 2019), https://www.law360.com/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware.

[35] *See* Maria Henriquez, *Iowa City Hospital Suffers Phishing Attack,* Security Magazine (Nov. 23, 2020), https://www.securitymagazine.com/articles/93988-iowa-city-hospital-suffers-phishing-attack.

[36] 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.

112. The American Medical Association ("AMA") has also warned healthcare companies about the importance of protecting their patients' confidential information:

> Cybersecurity is not just a technical issue; it's a patient safety issue. AMA research has revealed that 83% of physicians work in a practice that has experienced some kind of cyberattack. Unfortunately, practices are learning that cyberattacks not only threaten the privacy and security of patients' health and financial information, but also patient access to care.[37]

113. As implied by the above AMA quote, stolen Personal Information can be used to interrupt important medical services. This is an imminent and certainly impending risk for Plaintiff and Class Members.

114. Azura was on notice that the federal government has been concerned about healthcare company data encryption practices. Azura knew its employees accessed and utilized protected health information in the regular course of their duties, yet it appears that information was not encrypted.

115. The Office for Civil Rights ("OCR") urges the use of encryption of data containing sensitive personal information. As long ago as 2014, the Department fined two healthcare companies approximately two million dollars for failing to encrypt laptops containing sensitive personal information. In announcing the fines,

---

[37] Andis Robeznieks, *Cybersecurity: Ransomware attacks shut down clinics, hospitals*, American Medical Association (Oct. 4, 2019), https://www.ama-assn.org/practice-management/sustainability/cybersecurity-ransomware-attacks-shut-down-clinics-hospitals.

Susan McAndrew, OCR's deputy director of health information privacy, stated "[o]ur message to these organizations is simple: encryption is your best defense against these incidents."[38]

116. As a HIPAA covered business associate, Azura knew or should have known about its data security vulnerabilities and implemented enhanced and adequate protection, particularly given the nature of the Personal Information stored in its unprotected files.

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

117. Theft of PII/PHI is serious. The FTC warns consumers that identity thieves use PII/PHI to exhaust financial accounts, receive medical treatment, start new utility accounts, and incur charges and credit in a person's name.[39]

118. Identity thieves use personal information for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.[40]

---

[38] U.S. Department of Health and Human Services, *Stolen Laptops Lead to Important HIPAA Settlements* (Apr. 22, 2014), https://wayback.archive-it.org/3926/20170127085330/https://www.hhs.gov/about/news/2014/04/22/stolen-laptops-lead-to-important-hipaa-settlements.html.

[39] *See What to Know About Identity Theft*, Federal Trade Commission Consumer Advice, https://www.consumer.ftc.gov/articles/what-know-about-identity-theft (last accessed on Feb. 23, 2024).

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

According to Experian, one of the largest credit reporting companies in the world, "[t]he research shows that personal information is valuable to identity thieves, and if they can get access to it, they will use it" to among other things: open a new credit card or loan, change a billing address so the victim no longer receives bills, open new utilities, obtain a mobile phone, open a bank account and write bad checks, use a debit card number to withdraw funds, obtain a new driver's license or ID, and/or use the victim's information in the event of arrest or court action.[41]

119. With access to an individual's Personal Information, criminals can do more than just empty a victim's bank account—they can also commit all manner of fraud, including: obtaining a driver's license or official identification card in the victim's name but with the thief's picture, using the victim's name and Social Security number to obtain government benefits, or filing a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's Social Security number, rent a house, or receive medical services in the

number, alien registration number, government passport number, employer or taxpayer identification number." 12 C.F.R. § 1022.3(g).

[41] Susan Henson, *What Can Identity Thieves Do with Your Personal Information and How Can You Protect Yourself?*, Experian (Sept. 1, 2017), https://www.experian.com/blogs/ask-experian/what-can-identity-thieves-do-with-your-personal-information-and-how-can-you-protect-yourself/.

victim's name, and may even give the victim's personal information to police during an arrest, resulting in an arrest warrant being issued in the victim's name.[42]

120. Each year, identity theft causes tens of billions of dollars of losses to victims in the United States. For example, with the Personal Information stolen in the Data Breach, which includes Social Security numbers, identity thieves can open financial accounts, commit medical fraud, 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. These criminal activities have and will result in devastating financial and personal losses to Plaintiff and Class Members.

121. Personal Information is such a valuable commodity to identity thieves that once it has been compromised, criminals will use it and trade the information on dark web black markets for years.

122. For example, it is believed that certain highly sensitive personal information compromised in the 2017 Experian data breach was being used, three years later, by identity thieves to apply for COVID-19-related unemployment benefits.

---

[42] *See Warning Signs of Identity Theft*, Federal Trade Commission, https://www.identitytheft.gov/Warning-Signs-of-Identity-Theft (last visited Nov. 15, 2022).

123. The Personal Information exposed in this Data Breach is valuable to identity thieves for use in the kinds of criminal activity described herein. These risks are both certainly impending and substantial. As the FTC has reported, if cyber thieves get access to a person's highly sensitive information, they will use it.[43]

124. Cybercriminals 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.[44]

125. For instance, with a stolen Social Security number, which is only one subset of the Personal Information compromised in the Data Breach, someone can open financial accounts, get medical care, file fraudulent tax returns, commit crimes, and steal benefits.[45]

---

[43] Ari Lazarus, *How fast will identity thieves use stolen info?*, Federal Trade Commission (May 24, 2017), https://www.consumer.ftc.gov/blog/2017/05/how-fast-will-identity-thieves-use-stolen-info.

[44] *Report to Congressional Requesters: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, United States Government Accountability Office, https://www.gao.gov/assets/gao-07-737.pdf.

[45] *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-an-identity-thief-can-do-with-your-social-security-number-108597/.

126. Identity thieves can use Social Security numbers to obtain a driver's license or official identification card in the victim's name but with the thief's picture; use the victim's name and Social Security number to obtain government benefits; or file a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's Social Security number, rent a house or receive medical services in the victim's name, and may even give the victim's personal information to police during an arrest resulting in an arrest warrant being issued in the victim's name.

127. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "[c]ompared to credit card information, personally identifiable information and Social Security Numbers are worth more than 10x on the black market."

128. Identity theft is not an easy problem to solve. In a survey, the Identity Theft Resource Center found that most victims of identity crimes need more than a month to resolve issues stemming from identity theft and some need over a year.[46]

129. Theft of Social Security numbers also creates a particularly alarming situation for victims because those numbers cannot easily be replaced. In order to obtain a new number, a breach victim has to demonstrate ongoing harm from misuse

[46] *2021 Consumer Aftermath Report: How Identity Crimes Impact Victims, their Families, Friends, and Workplaces*, Identity Theft Resource Center (2021), https://www.idtheftcenter.org/identity-theft-aftermath-study/.

of his or her Social Security number, and a new identification number will not be provided until after the victim has suffered the harm.

130. Due to the highly sensitive nature of Social Security numbers, theft of Social Security numbers in combination with other PII (e.g., name, address, date of birth) is akin to having a master key to the gates of fraudulent activity. TIME quotes data security researcher Tom Stickley, who is employed by companies to find flaws in their computer systems, as stating, "If I have your name and your Social Security number and you haven't gotten a credit freeze yet, you're easy pickings."[47]

131. Theft of Personal Information is even more serious when it includes theft of PHI. Medical identity theft is one of the most common, most expensive, and most difficult-to-prevent forms of identity theft. According to Kaiser Health News, "medical-related identity theft accounted for 43 percent of all identity thefts reported in the United States in 2013," which is more than identity thefts involving banking and finance, the government and the military, or education.[48] "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

[47] Patrick Lucas Austin, *'It Is Absurd.' Data Breaches Show it's Time to Rethink How We Use Social Security Numbers, Experts Say*, TIME (Aug. 5, 2019), https://time.com/5643643/capital-one-equifax-data-breach-social-security/.
[48] Michael Ollove, "The Rise of Medical Identity Theft in Healthcare," Kaiser Health News (Feb. 7, 2014), https://khn.org/news/rise-of-indentity-theft/.

discover erroneous information has been added to their personal medical files due to the thief's activities."[49]

132. Data breaches involving medical information "typically leave[] a trail of falsified information in medical records that can plague victims' medical and financial lives for years."[50] It "is also more difficult to detect, taking almost twice as long as normal identity theft."[51] In warning consumers on the dangers of medical identity theft, the FTC states that an identity thief may use Personal Information "to see a doctor, get prescription drugs, buy medical devices, submit claims with your insurance provider, or get other medical care."[52] The FTC also warns, "If the thief's health information is mixed with yours, it could affect the medical care you're able to get or the health insurance benefits you're able to use. It could also hurt your credit."[53]

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

- Changes to their health care records, most often the addition of falsified information, through improper billing activity or activity by imposters.

[49] *Id.*
[50] Pam Dixon and John Emerson, *The Geography of Medical Identity Theft*, World Privacy Forum (Dec. 12, 2017), https://www.worldprivacyforum.org/2017/12/new-report-the-geography-of-medical-identity-theft/.
[51] *See* note 28, *supra*.
[52] *See* note 38, *supra*.
[53] *Id.*

These changes can affect the healthcare a person receives if the errors are not caught and corrected.

- Significant bills for medical goods and services not sought nor received.

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

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

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

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

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

- Sales of medical debt arising from identity theft can perpetuate a victim's debt collection and credit problems, through no fault of their own.[54]

134. There may also be a time lag between when sensitive personal information is stolen, when it is used, and when a person discovers it has been used. Fraud and identity theft resulting from the Data Breach may go undetected until debt collection calls commence months, or even years, later. An individual may not know

[54] *See* note 49, *supra*.

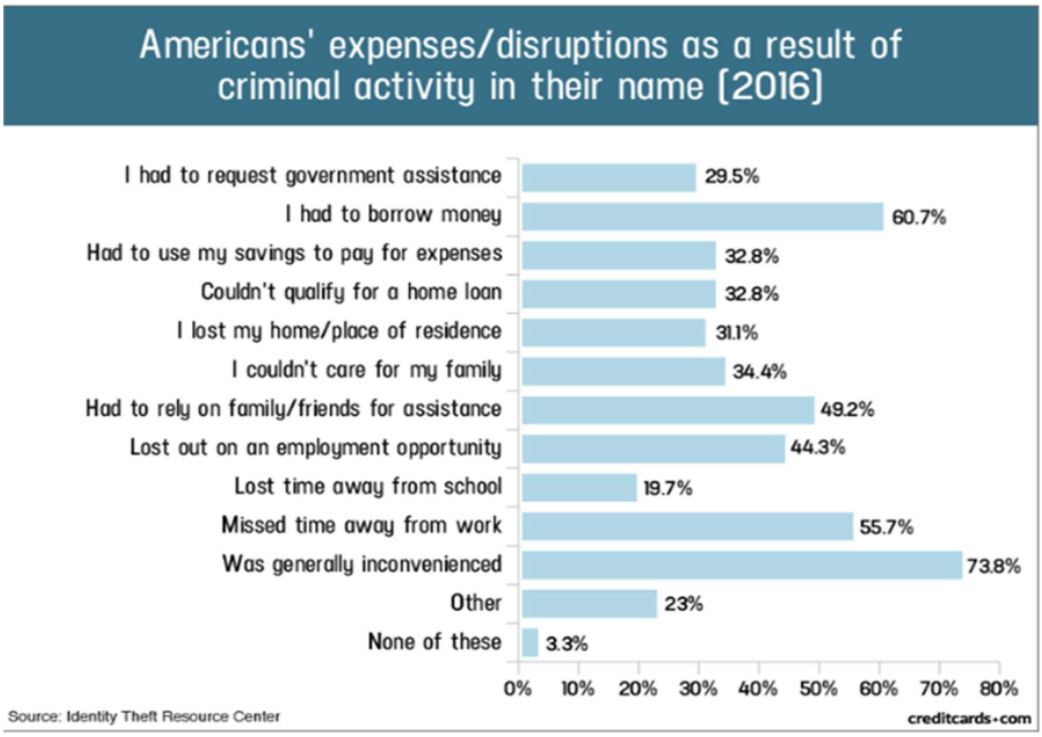
that his or her Social Security number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

135. For example, on average it takes approximately three months for consumers to discover their identity has been stolen and used, and it takes some individuals up to three years to learn that information.[55]

136. It is within this context that Plaintiff and all other Class Members must now live with the knowledge that their Personal Information is forever in cyberspace and was taken by people willing to use the information for any number of improper purposes and scams, including making the information available for sale on the black market.

137. A study by the Identity Theft Resource Center shows the multitude of harms caused by fraudulent use of personal and financial information:

[55] John W. Coffey, *Difficulties in Determining Data Breach Impacts*, 17 Journal of Systemics, Cybernetics and Informatics 9 (2019), http://www.iiisci.org/journal/pdv/sci/pdfs/IP069LL19.pdf.



138. Victims of the Data Breach, like Plaintiff and Class Members, must spend many hours and large amounts of money protecting themselves from the current and future negative impacts to their privacy and credit because of the Data Breach.[56]

139. As a direct and proximate result of the Data Breach, Plaintiff and Class Members have been placed at an imminent, immediate, and continuing increased risk of harm from fraud and identity theft. Plaintiff and Class Members must now take the time and effort (and spend the money) to mitigate the actual and potential impact of the Data Breach on their everyday lives, including purchasing identity

[56] *Guide for Assisting Identity Theft Victims*, Federal Trade Commission, (Sept. 2013), http://www.global-screeningsolutions.com/Guide-for-Assisting-ID-Theft-Victims.pdf.

theft and credit monitoring services every year for the rest of their lives, placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions and healthcare providers, closing or modifying financial accounts, and closely reviewing and monitoring bank accounts, credit reports, and health insurance account information for unauthorized activity for years to come.

140. Plaintiff and Class Members have suffered or will suffer actual harms for which they are entitled to compensation, including but not limited to the following:

a. Trespass, damage to, and theft of their personal property, including Private Information;

b. Improper disclosure of their Personal Information;

c. The imminent and certainly impending injury flowing from actual and potential future fraud and identity theft posed by their Personal Information being in the hands of criminals and having already been misused;

d. The imminent and certainly impending risk of having their confidential medical information used against them by spam callers to defraud them;

e. Damages flowing from Defendant's untimely and inadequate notification of the Data Breach;

f. Loss of privacy suffered as a result of the Data Breach;

g. Ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably expended to remedy or mitigate the effects of the data breach;

h. Ascertainable losses in the form of deprivation of the value of patients' personal information for which there is a well-established and quantifiable national and international market;

i. The loss of use of and access to their credit, accounts, and/or funds;

j. Damage to their credit due to fraudulent use of their Private Information; and

k. Increased cost of borrowing, insurance, deposits, and other items which are adversely affected by a reduced credit score.

141. Moreover, Plaintiff and Class Members have an interest in ensuring that their Personal Information, which remains in the possession of Defendant, is protected from further public disclosure by the implementation of better employee training and industry standard and statutorily compliant security measures and safeguards. Defendant has shown itself to be wholly incapable of protecting Plaintiff's and Class Members' Personal Information.

142. Because of the value of its collected and stored data, the medical industry has experienced disproportionally higher numbers of data theft events than

other industries. For this reason, Defendant knew or should have known about these dangers and strengthened its data security accordingly. Defendant was put on notice of the substantial and foreseeable risk of harm from a data breach, yet it failed to properly prepare for that risk.

J. The Data Breach Was Foreseeable and Preventable

143. Data disclosures and data breaches are preventable.[57] As Lucy Thompson wrote in the Data Breach and Encryption Handbook, "[i]n almost all cases, the data breaches that occurred could have been prevented by proper planning and the correct design and implementation of appropriate security solutions."[58] She added that "[o]rganizations that collect, use, store, and share sensitive personal data must accept responsibility for protecting the information and ensuring that it is not compromised . . . ."[59]

144. "Most of the reported data breaches are a result of lax security and the failure to create or enforce appropriate security policies, rules, and procedures … Appropriate information security controls, including encryption, must be implemented and enforced in a rigorous and disciplined manner so that a *data breach never occurs*."[60]

---

[57] Lucy L. Thompson, *Despite the Alarming Trends, Data Breaches Are Preventable*, Data Breach and Encryption Handbook (Lucy Thompson, ed., 2012).
[58] *Id.* at 17.
[59] *Id.* at 28.
[60] *Id.*

145. As explained by the Federal Bureau of Investigation, "[p]revention is the most effective defense against ransomware and it is critical to take precautions for protection."[61]

146. Plaintiff and Class Members entrusted their Personal Information to Azura as a condition of receiving healthcare-related services. Plaintiff and Class Members understood and expected that Azura or anyone in Azura's position would safeguard their Personal Information against cyberattacks, delete or destroy Personal Information that Azura was no longer required to maintain, and timely and accurately notify them if their Personal Information was compromised.

K. Plaintiff's and Class Members' Damages

147. To date, Azura has done nothing to provide Plaintiff and Class Members with relief for the damages they have suffered as a result of the Data Breach. Azura only offered credit monitoring services to "those who are eligible," but it did not disclose how it determined eligibility. Not only did Azura fail to provide any ongoing credit monitoring or identity protection services for all individuals impacted by the Data Breach, but the credit monitoring does nothing to compensate Class Members for damages incurred and time spent dealing with the Data Breach.

[61] *See How to Protect Your Networks from RANSOMWARE*, at 3, FBI.gov, https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view (last accessed Mar. 14, 2024).

148. Plaintiff and Class Members have been damaged by the compromise of their Personal Information in the Data Breach.

149. As a direct and proximate result of Azura's conduct, Plaintiff and Class Members have been placed at an imminent, immediate, and continuing increased risk of harm from fraud and identity theft. Plaintiff and Class Members face substantial risk of out-of-pocket fraud losses such as loans opened in their names, medical services billed in their names, tax return fraud, utility bills opened in their names, credit card fraud, and similar identity theft.

150. Plaintiff and Class Members face substantial risk of being targeted for future phishing, data intrusion, and other illegal schemes based on their Personal Information as potential fraudsters could use that information to target such schemes more effectively to Plaintiff and Class Members.

151. Plaintiff and Class Members have and will also incur out-of-pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breach.

152. Plaintiff and Class Members have suffered or will suffer actual injury as a direct result of the Data Breach. Many victims suffered ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach relating to:

a. Reviewing and monitoring financial and other sensitive accounts and finding fraudulent insurance claims, loans, and/or government benefits claims;

b. Purchasing credit monitoring and identity theft prevention;

c. Placing "freezes" and "alerts" with reporting agencies;

d. Spending time on the phone with or at financial institutions, healthcare providers, and/or government agencies to dispute unauthorized and fraudulent activity in their name;

e. Contacting financial institutions and closing or modifying financial accounts; and

f. Closely reviewing and monitoring Social Security Number, medical insurance accounts, bank accounts, and credit reports for unauthorized activity for years to come.

153. Plaintiff and Class Members suffered actual injury from having their Personal Information compromised as a result of the Data Breach including, but not limited to: (a) damage to and diminution in the value of their Personal Information, a form of property that Azura obtained from Plaintiff and Class Members; (b) violation of their privacy rights; (c) imminent and impending injury arising from the increased risk of identity theft and fraud; and (d) emotional distress.

154. Further, as a result of Defendant's conduct, Plaintiff and Class Members are forced to live with the anxiety that their Personal Information may be disclosed to the entire world, thereby subjecting them to embarrassment and depriving them of any right to privacy with respect to that information.

155. As a direct and proximate result of Defendant's actions and inactions, Plaintiff and Class Members have suffered a loss of privacy and are at a present and imminent and increased risk of future harm.

156. Moreover, Plaintiff and Class Members have an interest in ensuring that their Personal Information, which is believed to remain in the possession of Defendant, is protected from further breaches by the implementation of security measures and safeguards, including but not limited to, making sure that the storage of data or documents containing Personal Information is not accessible online, is properly encrypted, and that access to such data is password protected.

157. Many failures laid the groundwork for the occurrence of the Data Breach, starting with Defendant's failure to incur the costs necessary to implement adequate and reasonable cybersecurity training, procedures, and protocols that were necessary to protect Plaintiff's and Class Members' Personal Information.

158. Defendant maintained the Personal Information in an objectively reckless manner, making the Personal Information vulnerable to unauthorized disclosure.

159. Defendant knew, or reasonably should have known, of the importance of safeguarding Personal Information and of the foreseeable consequences that would result if Plaintiff's and Class Members' Personal Information was stolen, including the significant costs that would be placed on Plaintiff and Class Members as a result of the breach.

160. The risk of improper disclosure of Plaintiff's and Class Members' Personal Information was a known risk to Defendant, and thus Defendant was on notice that failing to take necessary steps to secure Plaintiff's and Class Members' Personal Information from that risk left the Personal Information in a dangerous condition.

161. Defendant disregarded the rights of Plaintiff and Class Members by, *inter alia*, (i) intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure that the Personal Information was protected against unauthorized intrusions; (ii) failing to disclose that it did not have adequately robust security protocols and training practices in place to adequately safeguard Plaintiff's and Class Members' Personal Information; (iii) failing to take standard and reasonably available steps to prevent the Data Breach; (iv) concealing the existence and extent of the Data Breach for an unreasonable duration of time; and (v) failing to provide Plaintiff and Class Members prompt and accurate notice of the Data Breach.

CLASS ALLEGATIONS

162. Plaintiff brings this class action individually and on behalf of all members of the following class of similarly situated persons pursuant to Federal Rule of Civil Procedure 23:

Nationwide Class

All persons in the United States whose Personal Information was compromised in the Data Breach disclosed by Azura on or about January 12, 2024, including all who were sent notice of the Data Breach.

163. Alternatively, or in addition to the nationwide class, Plaintiff seeks to represent the following state class:

Pennsylvania Class

All persons in the Commonwealth of Pennsylvania whose Personal Information was compromised in the Data Breach disclosed by Azura on or about January 12, 2024, including all who were sent notice of the Data Breach.

164. The nationwide class and the state class are collectively referred to as the "class." Excluded from the Class are Azura and its affiliates, parents, subsidiaries, officers, agents, and directors, as well as the judge(s) presiding over this matter and the clerks of said judge(s).

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

166. Numerosity: The members in the Class are so numerous that joinder of all Class Members in a single proceeding would be impracticable. As noted above, approximately 348,000 individuals' information was exposed in the Data Breach.

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

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

b. Whether they computer systems and data security practices employed by Azura to protect Plaintiff's and Class Members' Personal Information violated the FTC Act and/or HIPAA, and/or state laws and/or Azura's other duties discussed herein;

c. Whether Azura failed to adequately respond to the Data Breach, including failing to investigate it diligently and notify affected individuals in the most expedient time possible and without unreasonable delay, and whether this caused damages to Plaintiff and Class Members;

d. Whether Plaintiff and Class Members suffered injury as a proximate result of Azura's negligent actions or failures to act;

e. Whether Azura failed to exercise reasonable care to secure and safeguard Plaintiff's and Class Members' Personal Information;

f. Whether an implied contract existed between Class Members and Azura providing that Azura would implement and maintain reasonable security measures to protect and secure Class Members' Personal Information from unauthorized access and disclosure;

g. Whether injunctive relief is appropriate and, if so, what injunctive relief is necessary to redress the imminent and currently ongoing harm faced by Plaintiff and Class Members;

h. Whether Azura's actions and inactions alleged herein constitute gross negligence;

i. Whether Azura breached its duties to protect Plaintiff's and Class Members' Personal Information; and

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

168. Azura engaged in a common course of conduct giving rise to the legal rights sought to be enforced by Plaintiff individually and on behalf of all other Class

Members. Individual questions, if any, pale in comparison, in both quantity and quality, to the numerous common questions that dominate this action.

169. Typicality: Plaintiff's claims are typical of the claims of the Class. Plaintiff, like all proposed members of the Class, had Personal Information compromised in the Data Breach. Plaintiff and Class Members were injured by the same wrongful acts, practices, and omissions committed by Azura, as described herein. Plaintiff's claims therefore arise from the same practices or course of conduct that give rise to the claims of all Class Members.

170. Adequacy: Plaintiff will fairly and adequately protect the interests of the Class Members. Plaintiff is an adequate representative of the Class and has no interests adverse to, or in conflict with, the Class Plaintiff seeks to represent. Plaintiff has retained counsel with substantial experience and success in the prosecution of complex consumer protection class actions of this nature.

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

could afford individual litigation, the court system could not. Individualized litigation creates a potential for inconsistent or contradictory judgments, and increases the delay and expense to all parties and the court system. By contrast, the Class action device presents far fewer management difficulties and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court.

COUNT I
NEGLIGENCE

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

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

174. Azura knew, or should have known, the risks of collecting and storing Plaintiff's and Class Members' Personal Information and the importance of maintaining secure systems. Azura knew, or should have known, of the many data breaches that targeted healthcare providers in recent years.

175. Given the nature of Azura's business, the sensitivity and value of the Personal Information it maintains, and the resources at its disposal, Azura should have identified the vulnerabilities to its systems and prevented the Data Breach from occurring.

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

177. It was reasonably foreseeable to Azura that its failure to exercise reasonable care in safeguarding and protecting Plaintiff's and Class Members' Personal Information by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems would result in the unauthorized release, disclosure, and dissemination of Plaintiff's and Class Members' Personal Information to unauthorized individuals.

178. But for Azura's negligent conduct or breach of the above-described duties owed to Plaintiff and Class Members, their Personal Information would not have been compromised.

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

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

COUNT II
NEGLIGENCE PER SE

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

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

182. Azura's duties also arise from Section 5 of the FTC Act ("FTCA"), 15 U.S.C. § 45(a)(1), which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted by the FTC, the unfair act or practice by a business, such as

Azura, of failing to employ reasonable measures to protect and secure Private Information.

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

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

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

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

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

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

189. It was reasonably foreseeable to Azura that its failure to exercise reasonable care in safeguarding and protecting Plaintiff's and Class Members' Personal Information by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems, would result in the release, disclosure, and dissemination of Plaintiff's and Class Members' Personal Information to unauthorized individuals.

190. The injury and harm that Plaintiff and the other Class Members suffered was the direct and proximate result of Azura's violations of HIPAA Privacy and Security Rules and Section 5 of the FTCA. Plaintiff and Class Members have suffered (and will continue to suffer) economic damages and other injury and actual harm in the form of, *inter alia*: (i) a substantially increased risk of identity theft and medical theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (ii) improper disclosure of their Personal Information; (iii) breach of the confidentiality of their Personal Information; (iv) deprivation of the value of their Personal Information, for which there is a well-established national and international market; (v) lost time and money incurred to

mitigate and remediate the effects of the Data Breach, including the increased risks of medical identity theft they face and will continue to face; and (vi) actual or attempted fraud.

COUNT III
BREACH OF FIDUCIARY DUTY

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

192. Plaintiff and Class Members either directly or indirectly gave Azura their Personal Information in confidence, believing that Azura would protect that information. Plaintiff and Class Members would not have provided Azura with this information had they known it would not be adequately protected. Azura's acceptance and storage of Plaintiff's and Class Members' Personal Information created a fiduciary relationship between Azura and Plaintiff and Class Members. In light of this relationship, Azura must act primarily for the benefit of its patients and health plan participants, which includes safeguarding and protecting Plaintiff's and Class Members' Personal Information.

193. Azura has a fiduciary duty to act for the benefit of Plaintiff and Class Members upon matters within the scope of their relationship. It breached that duty by failing to properly protect the integrity of the system containing Plaintiff's and Class Members' Personal Information, failing to comply with the data security

guidelines set forth by HIPAA, and otherwise failing to safeguard the Personal Information of Plaintiff and Class Members it collected.

194. As a direct and proximate result of Azura's breaches of its fiduciary duties, Plaintiff and Class Members have suffered and will suffer injury, including, but not limited to: (i) a substantial increase in the likelihood of identity theft; (ii) the compromise, publication, and theft of their Personal Information; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from unauthorized use of their Personal Information; (iv) lost opportunity costs associated with effort attempting to mitigate the actual and future consequences of the Data Breach; (v) the continued risk to their Personal Information, which remains in Azura's possession; (vi) future costs in terms of time, effort, and money that will be required to prevent, detect, and repair the impact of the Personal Information compromised as a result of the Data Breach; and (vii) actual or attempted fraud.

COUNT IV
BREACH OF IMPLIED CONTRACT

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

196. Defendant required Plaintiff and Class Members to provide, or authorize the transfer of, their Personal Information in order for Azura to provide services. In exchange, Defendant entered into implied contracts with Plaintiff and Class Members in which Defendant agreed to comply with its statutory and common

law duties to protect Plaintiff's and Class Members' Personal Information and to timely notify them in the event of a data breach.

197. Plaintiff and Class Members would not have provided their Personal Information to Defendant, or would not have agreed to have that information provided to Defendant, had they known that Defendant would not safeguard their Personal Information, as promised, or provide timely notice of a data breach.

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

199. Defendant breached the implied contracts by failing to safeguard Plaintiff's and Class Members' Personal Information and by failing to provide them with timely and accurate notice of the Data Breach.

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

COUNT V
UNJUST ENRICHMENT

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

202. This claim is pleaded in the alternative pursuant to Fed. R. Civ. P. 8(d).

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

204. Azura accepted or had knowledge of the benefits conferred upon it by Plaintiff and Class Members. Azura also benefitted from the receipt of Plaintiff's and Class Members' PHI.

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

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

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

COUNT VI
BREACH OF CONFIDENCE

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

209. Plaintiff and Class Members have an interest, both equitable and legal, in the Personal Information about them that was conveyed or provided to, collected

by, and maintained by Azura, and that was ultimately accessed or compromised in the Data Breach.

210. As a healthcare provider, Azura has a special relationship to its patients and other affiliated persons, such as Plaintiff and the Class Members.

211. Because of that special relationship, Azura was provided with and stored private and valuable PHI and other Personal Information related to Plaintiff and the Class, which it was required to maintain in confidence.

212. Plaintiffs and the Class provided Azura with their Personal Information under both the express and/or implied agreement of Azura to limit the use and disclosure of such information.

213. Azura owed a duty to Plaintiff and the Class Members to exercise the utmost care in obtaining, retaining, securing, safeguarding, deleting, and protecting their Personal Information in its possession from being compromised, lost, stolen, accessed by, misused by, or disclosed to unauthorized persons.

214. Azura had an obligation to maintain the confidentiality of Plaintiff's and the Class Members' Personal Information.

215. Plaintiff and the Class have a privacy interest in their personal medical matters, and Azura had a duty not to disclose confidential medical information and records concerning its patients.

216. As a result of the parties' relationship, Azura had possession and knowledge of the confidential Personal Information and confidential medical records of Plaintiff and the Class.

217. Plaintiff's and Class Members' Personal Information is not generally known to the public and is confidential by nature.

218. Plaintiff and Class Members did not consent to nor authorize Azura to release or disclose their Personal Information to an unknown threat actor.

219. Azura breached the duties of confidence it owed to Plaintiff and the Class when Plaintiff's and Class Members' Personal Information was disclosed to unknown criminal hackers.

220. Azura breached its duties of confidence by failing to safeguard Personal Information, including by, among other things: (a) mismanaging its system and failing to identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that resulted in the unauthorized access and compromise of PII and PHI; (b) mishandling its data security by failing to assess the sufficiency of its safeguards in place to control these risks; (c) designing and implementing inadequate cybersecurity safeguards and controls; (d) failing to adequately test and monitor the effectiveness of the safeguards' key controls, systems, and procedures; (e) failing to evaluate and adjust its information security program in light of the circumstances alleged herein;

(f) failing to detect the breach at the time it began or within a reasonable time thereafter; (g) failing to follow its own privacy policies and practices published to its patients; (h) storing PHI and medical records/information in an unencrypted and vulnerable manner, allowing its disclosure to hackers; and (i) making an unauthorized and unjustified disclosure and release of Plaintiff's and Class Members' Personal Information, inclusive of medical records/information, to a criminal third party.

221. But for Azura's wrongful breach of its duty of confidences owed to Plaintiff and the Class Members, their privacy, confidences, and Personal Information would not have been compromised.

222. As a direct and proximate result of Azura's breach of confidences, Plaintiff and the Class have suffered and/or are at a substantial increased risk of suffering injuries, including:

a. The erosion of the essential and confidential relationship between Azura—as a healthcare services provider—and Plaintiff and the Class as patients;

b. Loss of the privacy and confidential nature of their PHI;

c. Theft of their PII and/or PHI;

d. Costs associated with the detection and prevention of identity theft or medical identity theft;

e. Costs associated with purchasing credit monitoring and identity theft protection services;

f. Lowered credit scores resulting from credit inquiries following fraudulent activities;

g. Costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Data Breach—including finding fraudulent charges, cancelling and reissuing cards, enrolling in credit monitoring and identity theft protection services, freezing and unfreezing accounts, and imposing withdrawal and purchase limits on compromised accounts;

h. The imminent and certain impending injury flowing from the increased risk of potential fraud and identity theft posed by their PII and/or PHI being placed in the hands of criminals;

i. Damages to and diminution in value of their PII and PHI entrusted, directly or indirectly, to Azura with the mutual understanding that Azura would safeguard Personal Information against theft and not allow access and misuse of their data by others;

j. Continued risk of exposure to hackers and thieves of their PII and/or PHI, which remains in Azura's possession and is subject to further breaches so long as Azura fails to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' data;

k. Loss of personal time spent carefully reviewing statements from health insurers and providers to check for charges for services not received, as directed to do by Azura; and

l. Mental anguish accompanying the loss of confidences and disclosure of their confidential and private PHI.

223. Additionally, Azura received payments from Plaintiff and Class Members for services with the understanding that Azura would uphold its responsibilities to maintain the confidences of Plaintiff's and Class Members' private information.

224. Azura breached the confidence of Plaintiff and the Class Members when it made an unauthorized release and disclosure of their Personal Information and, accordingly, it would be inequitable for Azura to retain the benefit at Plaintiff's and Class Members' expense.

225. As a direct and proximate result of Azura's breach of its duty, Plaintiff and Class Members are entitled to damages, including compensatory, punitive,

and/or nominal damages, and/or disgorgement or restitution, in an amount to be proven at trial.

COUNT VII
DECLARATORY AND INJUNCTIVE RELIEF

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

227. This count is brought under the Federal Declaratory Judgment Act, 28 U.S.C. § 2201.

228. Defendant owes a duty of care to Plaintiff and Class Members that require it to adequately secure Plaintiff's and Class Members' Personal Information.

229. Defendant still possesses the Personal Information of Plaintiff and Class Members.

230. Defendant has not satisfied its contractual obligations and legal duties to Plaintiff and Class Members.

231. Actual harm has arisen in the wake of the Data Breach regarding Defendant's contractual obligations and duties of care to provide security measures to Plaintiff and Class Members. Further, Plaintiff and Class Members are at risk of additional or further harm due to the exposure of their Personal Information and Defendant's failure to address the security failings that led to such exposure.

232. There is no reason to believe that Defendant's employee training and security measures are any more adequate now than they were before the breach to meet Defendant's contractual obligations and legal duties.

233. Plaintiff, therefore, seeks a declaration (1) that Defendant's existing data security measures do not comply with its contractual obligations and duties of care to provide adequate data security, and (2) that to comply with its contractual obligations and duties of care, Defendant must implement and maintain reasonable security measures, including, but not limited to, the following:

a. Ordering that Defendant engage internal security personnel to conduct testing, including audits on Defendant's systems, on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

b. Ordering that Defendant engage third-party security auditors and internal personnel to run automated security monitoring;

c. Ordering that Defendant audit, test, and train its security personnel and employees regarding any new or modified data security policies and procedures;

d. Ordering that Defendant purge, delete, and destroy, in a reasonably secure manner, any Private Information not necessary for its provision of services;

e. Ordering that Defendant conduct regular database scanning and security checks; and

f. Ordering that Defendant routinely and continually conduct internal training and education to inform internal security personnel and employees how to safely share and maintain highly sensitive personal information, including but not limited to, patient personally identifiable information and patient protected health information.

PRAYER FOR RELIEF

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

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

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

C. Awarding Plaintiff and the Class equitable, injunctive, and declaratory relief, as may be appropriate. Plaintiff, individually and on behalf of the Class, seeks appropriate injunctive relief designed to prevent Azura from experiencing another data breach by adopting and implementing best data security practices to safeguard

Personal Information and to provide or extend credit monitoring services and similar services to protect against all types of identity theft and medical identity theft;

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

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

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

JURY TRIAL DEMANDED

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

Dated: March 15, 2024

Respectfully submitted,

/s/ Andrew W. Ferich

Andrew W. Ferich (PA 313696)
Chloe R. DeOnna (PA 330351)
AHDOOT & WOLFSON, PC
201 King of Prussia Road, Suite 650
Radnor, PA 19087
Telephone: (310) 474-9111
Facsimile: (310) 474-8585
aferich@ahdootwolfson.com
cdeonna@ahdootwolfson.com

Counsel for Plaintiff and the Putative Class

ClassAction.org