IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF PENNSYLVANIA

STEVEN GRAVLEY, SR., TYRONE BANKS, and BARBARA WELZENBACH, individually and on behalf of all others similarly situated, Plaintiffs, v. FRESENIUS VASCULAR CARE, INC. d/b/a AZURA VASCULAR CARE, Defendant.	Case No. 2:24-cv-01148-MMB **CONSOLIDATED CLASS ACTION COMPLAINT** CLASS ACTION JURY TRIAL DEMANDED

Plaintiffs Steven Gravley, Sr., Tyrone Banks, and Barbara Welzenbach ("Plaintiffs"), individually and on behalf of all others similarly situated, by and through the undersigned attorneys, bring this class action against Defendant Fresenius Vascular Care, Inc. d/b/a Azura Vascular Care ("Azura" or "Defendant") and complain and allege upon personal knowledge as to their own actions and their counsels' investigations, and upon information and good faith belief as to all other matters, as follows:

INTRODUCTION

1. Plaintiffs bring 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 348,000 current and former patients, or other persons affiliated with Azura.

2. 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 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 Azura with sensitive Personal Information. By being entrusted with this sensitive information, Azura assumes a legal duty to reasonably safeguard it.

4. Starting on or before September 27, 2023, an unauthorized third party accessed Azura's computer systems.[1] On November 9, 2023, Azura confirmed that some of its information had been affected by a cybersecurity incident (the "Data Breach"). Azura conducted an incident response with the assistance of a third-party forensic firm and reported that 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 ("SSN"), 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.[2]

7. On or around January 12, 2024, Azura sent a Notice of Data Breach (the "Notice Letter") informing breach victims of the following:

> On November 9, 2023, Azura confirmed that some of its information had been affected by a cybersecurity incident. Azura conducted incident response and recovery procedures, took steps to contain the incident, and investigated with the assistance of a third-party forensic firm. Based on information learned to date, we believe that starting on or before September 27, 2023, the attacker(s) accessed certain systems and encrypted certain files. On November 15, 2023, we confirmed that these files included personal information for some of our patients. At this time,

[1] *Important Notice for Patients of Azura Vascular Care*, available at: https://www.azuravasculararcare.com/notice/ (last accessed on May 30, 2024).
[2] *Id.*

we have no evidence that the personal information was taken or has been misused.[3]

8. The Notice Letter acknowledges that Plaintiffs' and class members' Personal Information was unlawfully accessed and encrypted by the cyber criminals, but Azura did not disclose how Azura discovered the 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 it determined that the PII/PHI had been "accessed" by the unauthorized actor, and, importantly, what specific steps it took following the Data Breach to secure its systems and prevent future cyberattacks.

9. 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.

10. Plaintiffs bring this class action lawsuit on behalf of themselves and those similarly situated to address Azura's inadequate safeguarding of Plaintiffs and class members' Personal Information that it collected and maintained, and for failing to provide adequate notice to Plaintiffs and class members.

11. Plaintiffs bring claims for negligence, negligence per se, breach of fiduciary duty, breach of implied contract, unjust enrichment, violations of consumer protection laws, breach of confidence, and declaratory and injunctive relief. To remedy these violations of law, Plaintiffs 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.

[3] *Id.*

PARTIES

Plaintiffs

Plaintiff Steven Gravley, Sr.

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

13. Plaintiff is 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 undertook a duty to act reasonably in its handling of his Personal Information. On information and belief, Azura did not take proper care of Plaintiff's Personal Information, leading to its exposure by cybercriminals as a direct result of its inadequate security measures. In close proximity to the Data Breach, and within a few months after the breach, Plaintiff believes he suffered medical identity theft as he received an unfamiliar medical bill.

14. Plaintiff Gravley is very careful about sharing his sensitive Personal Information. Plaintiff Gravley has never knowingly transmitted unencrypted sensitive Personal Information over the internet or any other unsecured source.

15. As a result of the Data Breach, Plaintiff Gravley spent time dealing with the consequences of the Data Breach, which includes time spent verifying the legitimacy of the Notice of Data Breach. This time has been lost forever and cannot be recaptured.

16. 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 Gravley will need to maintain these heightened measures for years.

17. Plaintiff Gravley 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 Gravley's confidential personal information—a form of intangible property that Plaintiff Gravley entrusted to Azura, which was compromised as a result of the Data Breach it failed to prevent and (b) a violation of Plaintiff Gravley's privacy rights as a result of Azura's unauthorized disclosure of Personal Information.

18. Had Plaintiff Gravley known that Azura does not adequately protect PII/PHI, Plaintiff Gravley would not have used Azura's services and agreed to provide Azura with PII/PHI.

19. Plaintiff Gravley suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of his privacy.

20. Defendant's Notice Letter admits that Plaintiff Gravley's Personal Information was encrypted and obtained by criminal third parties. Thus, Plaintiff Gravley's and class members' information is already being misused by cybercriminals.

21. Plaintiff Gravley has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from his Personal Information being placed in the hands of unauthorized third parties and possibly criminals.

22. As a result of Azura's failure to adequately safeguard Plaintiff Gravley's information, he has been injured. Plaintiff Gravley is also at a continued risk of harm because upon information and belief 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.

Plaintiff Tyrone Banks

23. Plaintiff Tyrone Banks is a resident and citizen of Chicago, Illinois.

24. Plaintiff Banks is and/or has been a patient at Azura Vascular Care at its location on Pasquinelli Drive in Westmont, Illinois. Plaintiff Banks provided PII/PHI to Azura in connection with receiving healthcare services from Azura. In receiving Plaintiff Banks's Personal Information for its business purposes, Azura undertook a duty to act reasonably in its handling of his Personal Information. Azura did not take proper care of Plaintiff Banks's Personal Information, leading to its exposure by cybercriminals as a direct result of its inadequate security measures.

25. On or around January 12, 2024, Azura notified Plaintiff Banks that Defendant's network had been accessed and Plaintiff Banks's Personal Information may have been involved in the Data Breach.

26. As a result of the Data Breach, Plaintiff Banks spent time dealing with the consequences of the Data Breach, which includes time spent verifying the legitimacy of the Notice of Data Breach, self-monitoring his accounts and credit reports to ensure no fraudulent activity has occurred and freezing his own credit. This time has been lost forever and cannot be recaptured. Plaintiff Banks has spent significant time over the course of several weeks engaging in monitoring and other mitigation efforts.

27. Plaintiff Banks suffered actual injury in the form of unauthorized charges made by an unknown party to his personal debit card on or around November 27, 2023. Plaintiff Banks spent time mitigating the effects of these unauthorized charges to his debit card, namely taking the time to dispute the unauthorized charges with Plaintiff Banks's bank, as well as going through the process to order a replacement debit card. Plaintiff Banks was also without use of his debit card while he awaited a replacement.

28. 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 Banks will need to maintain these heightened measures for years.

29. Plaintiff Banks 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 Banks's confidential personal information—a form of intangible property that Plaintiff Banks entrusted to Azura, which was compromised as a result of the Data Breach it failed to prevent and (b) a violation of Plaintiff Banks's privacy rights as a result of Azura's unauthorized disclosure of Personal Information.

30. Had Plaintiff known that Azura does not adequately protect PII/PHI, Plaintiff Banks would not have used Azura's services and agreed to provide Azura with PII/PHI.

31. Plaintiff Banks suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of his privacy.

32. Defendant's Notice Letter admits that Plaintiff Banks's Personal Information was encrypted and obtained by criminal third parties. Thus, Plaintiff Banks's and class members' information is already being misused by cybercriminals.

33. Plaintiff Banks has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from his Personal Information being placed in the hands of unauthorized third parties and possibly criminals.

34. As a result of Azura's failure to adequately safeguard Plaintiff Banks's information, Plaintiff has been injured. Plaintiff Banks is also at a continued risk of harm because upon information and belief 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.

Plaintiff Barbara Welzenbach

35. Plaintiff Barbara Welzenbach is a resident and citizen of Baltimore, Maryland.

36. Plaintiff Welzenbach was a patient at Azura Vascular Care at its location at the Franklin Square Hospital in Baltimore, Maryland. Plaintiff Welzenbach provided PII/PHI to Azura in connection with receiving healthcare services from Azura. In receiving Plaintiff Welzenbach's Personal Information for its business purposes, Azura undertook a duty to act reasonably in its handling of his Personal Information. Azura did not take proper care of Plaintiff Welzenbach's Personal Information, leading to its exposure by cybercriminals as a direct result of its inadequate security measures.

37. On or around January 12, 2024, Azura notified Plaintiff Welzenbach that Defendant's network had been accessed and Plaintiff Welzenbach's Personal Information may have been involved in the Data Breach.

38. As a result of the Data Breach, Plaintiff Welzenbach spent time dealing with the consequences of the Data Breach, which includes time spent verifying the legitimacy of the Notice of Data Breach, and self-monitoring her accounts and credit reports to ensure no fraudulent activity has occurred. This time has been lost forever and cannot be recaptured. Plaintiff Welzenbach has spent approximately 20 hours engaging in monitoring and other mitigation efforts.

39. Plaintiff Welzenbach suffered actual injury in the form of suspected identity theft, as, since the Data Breach, she has received multiple offers of car insurance for a car she does not own. Plaintiff Welzenbach has never driven a car. Plaintiff Welzenbach spent time investigating and mitigating the effects of the suspected identity theft by calling the Department of Motor Vehicles. Plaintiff has also noticed a noticeable uptick in spam and phishing emails, calls, and text messages since the Data Breach.

40. 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 Welzenbach will need to maintain these heightened measures for years.

41. Plaintiff Welzenbach 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 Welzenbach's confidential personal information—a form of intangible property that Plaintiff Welzenbach entrusted to Azura, which was compromised as a result of the Data Breach it failed to prevent and (b) a violation of Plaintiff Welzenbach's privacy rights as a result of Azura's unauthorized disclosure of Personal Information.

42. Had Plaintiff Welzenbach known that Azura does not adequately protect PII/PHI, Plaintiff Welzenbach would not have used Azura's services and agreed to provide Azura with PII/PHI.

43. Plaintiff Welzenbach suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of her privacy.

44. Defendant's Notice Letter admits that Plaintiff Welzenbach's Personal Information was encrypted and obtained by criminal third parties. Thus, Plaintiff Welzenbach's and class members' information is already being misused by cybercriminals.

45. Plaintiff Welzenbach has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from her Personal Information being placed in the hands of unauthorized third parties and possibly criminals.

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

risk of harm because upon information and belief 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

47. 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.[4]

48. According to its website, Azura presently operates 70 outpatient vascular centers and ambulatory surgery centers in approximately 25 states (and Puerto Rico) throughout the United States, including three locations in the Commonwealth of Pennsylvania and one location in Illinois.

JURISDICTION AND VENUE

49. 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.

[4] *Fresenius Vascular Care Announces New Name to Reflect Company's Strategic Transformation*, AzuraVascularcare.com (June 20, 2017), https://www.azuravascularcare.com/in-the-news/fresenius-vascular-care-announces-new-name/.

50. 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.

51. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(b)(1) because a substantial part of the events giving rise to this action occurred in this District. Moreover, Azura resides in this district, maintains Plaintiffs' and class members' Personal Information in this district, and this district is where a substantial part of the acts, omissions, and events giving rise to Plaintiffs' claims occurred.

FACTUAL ALLEGATIONS

A. Overview of Azura Health

52. 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.

53. 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.

54. As a regular part of its business, Azura requires patients to provide personal information before it provides them services. That information includes, but is not limited to:

a. name,

b. address,

c. phone number and email address;

d. date of birth;

e. demographic information;

f. SSN;

g. financial information;

h. information relating to individual medical history;

i. information concerning an individual's doctor, nurse, or other medical providers;

j. medication information;

k. health insurance information;

l. photo identification; and

m. other information that Azura may deem necessary to provide its services.

55. Azura stores this information digitally. Additionally, Azura may receive Personal Information from other individuals and/or organizations that are part of a patient's "circle of care," such as referring physicians, customers' other doctors, customers' health plan(s), guarantors, close friends, and/or family members.

56. 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[5] 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.

[5] 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.

57. In its Privacy Statement, Azura affirms that it "value[s] your trust and [is] committed to the responsible management of Personal Information,"[6] 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."[7]

58. Yet, Azura maintained inadequate security measures which allowed the Data Breach to occur. It then waited nearly two months after discovering the Data Breach to disclose that patient PII/PHI had been compromised.

59. Plaintiffs 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.

60. Because of the highly sensitive and personal nature of the information Azura acquires and stores with respect to its healthcare entities' patients and other individuals, Plaintiffs and class members reasonably expect that Azura will, among other things: keep their Personal Information confidential; comply with healthcare industry standards related to data security and Personal Information; inform them of legal duties and comply with all federal and state laws protecting their Personal Information; only use and release their Personal Information for reasons that relate to medical care and treatment; and provide adequate notice to them if their Personal Information is disclosed without authorization.

B. Azura Is a HIPAA Covered Business Entity

61. Azura is a HIPAA covered business entity that provides healthcare services to patients. As a condition of receiving Azura's services, Azura requires that patients, including

[6] *Privacy Statement*, Fresenius Medical Care (July 20, 2023), https://fmcna.com/privacy-statement/.
[7] *HIPAA Notice of Privacy Practices*, Fresenius Medical Care (Apr. 26, 2022), https://fmcna.com/notice-of-privacy-practices/.

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

62. 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, 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.

63. 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."[8]

64. Plaintiffs 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. Plaintiffs and class members reasonably expected that Azura would safeguard their highly sensitive information and keep their Personal Information confidential.

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

65. According to the Notice Letter provided by Azura to Plaintiffs and class members, Azura was subject to a cybersecurity attack beginning on or before September 27, 2023.

66. On November 9, 2023, Azura discovered that the Data Breach may have impacted

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

Personal Information stored in its systems and encrypted files.

67. In response, Azura stated that it "conducted incident response and recovery procedures, took steps to contain the incident, and investigated with the assistance of a third-party forensic firm."[9]

68. 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, SSNs, insurance policy and guarantor information, diagnosis and treatment information, and other information from medical or billing records.

69. Azura did not publicly announce the Data Breach until two months later, on January 12, 2024.[10] 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.[11]

70. 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 Plaintiffs and class members, what actual steps Azura took following the Data Breach to secure its systems and train its employees to prevent further cyberattacks.

71. Based on Azura's acknowledgment that Personal Information was accessed by an

[9] *See* "Notice Letter," note 1, *supra.*
[10] *Id.*
[11] *Id*.

unauthorized party, it is evident that unauthorized criminal actors did, in fact, access Azura's network Plaintiffs' and class members' Personal Information in an attack designed to acquire that sensitive, confidential, and valuable information.

72. 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.

73. 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.[12]

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

75. 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 Plaintiffs and class members.

76. Due to Azura's inadequate security measures, Plaintiffs and class members now face a present, immediate, and ongoing risk of fraud and identity theft and must deal with that threat forever.

77. Azura had obligations created by HIPAA, contract, industry standards, and common law to Plaintiffs and class members to keep their Personal Information confidential and to protect it from unauthorized access and disclosure.

78. Plaintiffs and class members entrusted their Personal Information to Azura, or

[12] *Cases Currently Under Investigation*, U.S. Department of Health and Human Services, https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (last accessed May 30, 2024).

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.

79. By obtaining, collecting, using, and deriving a benefit from Plaintiffs' and class members' Personal Information, Azura assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiffs' and class members' Personal Information from unauthorized disclosure.

80. Plaintiffs and the class members have taken reasonable steps to maintain the confidentiality of their personal information. Plaintiffs 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.

81. As a result of Azura's negligent and wrongful conduct, Plaintiffs' and class members' highly confidential and sensitive Personal Information was left exposed to cybercriminals. The unencrypted Personal Information of Plaintiffs and class members will end up for sale to identity thieves on the dark web, if it has not already, or it could simply fall into the hands of companies that will use the detailed Personal Information for targeted marketing without the approval of Plaintiffs and class members. Unauthorized individuals can now easily access the Personal Information of Plaintiffs and class members.

D. Azura Failed to Comply with HIPAA Requirements

82. 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.

83. Azura is subject to the rules and regulations for safeguarding electronic forms of medical information pursuant to the Health Information Technology Act ("HITECH").[13] *See* 42 U.S.C. §17921, 45 C.F.R. § 160.103.

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

85. 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.

86. 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.

87. "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.

88. 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;

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

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

d. Ensure compliance by its workforce.

89. 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).

90. 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).

91. 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.

92. 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*."[14]

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

[14] *Breach Notification Rule*, U.S. Department of Health & Human Services, https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html (last accessed on May 21, 2024) (emphasis added).

94. 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).

95. 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.[15] 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 for securing e-PHI." U.S. Department of Health & Human Services, Guidance on Risk Analysis.[16]

E. Azura Failed to Follow FTC Guidelines

96. 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

[15] *Security Rule Guidance Material*, U.S. Department of Health & Human Services, http://www.hhs.gov/hipaa/for-professionals/security/guidance/index.html (last accessed on May 21, 2024).

[16] *Guidance on Risk Analysis*, U.S. Department of Health & Human Services, https://www.hhs.gov/hipaa/for-professionals/security/guidance/guidance-risk-analysis/index.html (last accessed on May 21, 2024).

"unfair practice" in violation of the FTC Act. *See, e.g., FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015).

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

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

99. 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.

100. The FTC further recommends that companies not maintain personal 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.

101. 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.

102. These FTC enforcement actions include actions against healthcare providers and partners like Azura. *See, e.g., In the Matter of Labmd, Inc., A Corp*, 2016-2 Trade Cas. (CCH) ¶ 79708, 2016 WL 4128215, at *32 (MSNET July 28, 2016) ("[T]he Commission concludes that LabMD's data security practices were unreasonable and constitute an unfair act or practice in violation of Section 5 of the FTC Act.").

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

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

105. Azura was at all times fully aware of its obligation to protect the Personal Information of the patients and plan members about whom it stored Personal 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

106. 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.

107. 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.

108. 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.

109. 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.

110. 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 Plaintiffs and Class Members a Duty to Safeguard Their Personal Information

111. In addition to its obligations under federal and state laws, Azura owed a duty to Plaintiffs 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 Plaintiffs 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 Plaintiffs and class members.

112. Azura owed a duty to Plaintiffs 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 Personal Information within its computer systems on how to adequately protect Personal Information.

113. Azura owed a duty to Plaintiffs and class members to implement processes that would detect a compromise of Personal Information in a timely manner.

114. Azura owed a duty to Plaintiffs and class members to act upon data security warnings and alerts in a timely fashion.

115. Azura owed a duty to Plaintiffs and class members to disclose in a timely and accurate manner when and how the Data Breach occurred.

116. Azura owed a duty of care to Plaintiffs and class members because they were foreseeable and probable victims of any inadequate data security practices.

117. Azura breached its obligations to Plaintiffs and class members and/or was otherwise negligent and reckless because it failed to properly maintain and safeguard its computer systems and data and failed to audit, monitor, or ensure the integrity of its vendor's data security practices. Azura's unlawful conduct includes, but is not limited to, the following acts and/or omissions:

a. Failing to maintain an adequate data security system that would reduce the risk of data breaches and cyberattacks;

b. Failing to adequately protect its patients' Personal Information;

c. Failing to properly monitor its own data security systems for existing intrusions;

d. Failing to audit, monitor, or ensure the integrity of its vendor's data security practices;

e. Failing to sufficiently train its employees and vendors regarding the proper handling of its patients' Personal Information;

f. Failing to fully comply with FTC guidelines for cybersecurity in violation of the FTCA;

g. Failing to adhere to HIPAA guidelines and industry standards for cybersecurity as discussed above; and

h. Otherwise breaching its duties and obligations to protect Plaintiffs' and class members' Personal Information.

118. Azura negligently and unlawfully failed to safeguard Plaintiffs' and class members' Personal Information by allowing cyberthieves to access its computer network and systems which contained unsecured and unencrypted Personal Information.

119. Had Azura remedied the deficiencies in its information storage and security systems or those of its vendors and affiliates, followed industry guidelines, and adopted security measures recommended by experts in the field, it could have prevented intrusion into its information storage and security systems and, ultimately, the theft of Plaintiffs' and class members' confidential Personal Information.

H. Azura Knew That Criminals Target PII/PHI from Healthcare Entities

120. 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.

121. In light of recent high profile cybersecurity incidents at other healthcare partner and provider companies, including HCA Healthcare (11 million patients, July 2023), Managed Care of North America (8 million patients, March 2023), PharMerica Corporation (5 million patients,

March 2023), HealthEC LLC (4 million patients, July 2023), ESO Solutions, Inc. (2.7 million patients, September 2023), and Prospect Medical Holdings, Inc. (1.3 million patients, July-August 2023), Defendant knew or should have known that its electronic medical records would be targeted by cybercriminals.

122. At all relevant times, Azura knew, or should have known, its patients', Plaintiffs', 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 Plaintiffs' and class members' Personal Information from cyberattacks that Azura should have anticipated and guarded against.

123. "Hospitals store an incredible amount of patient data. Confidential data that's worth a lot of money to hackers who can sell it on easily – making the industry a growing target."[17]

124. Cybercriminals seek out PHI at a greater rate than other sources of personal information. In a 2023 report, the healthcare compliance company Protenus found there were 956 medical data breaches in 2022 with over 59 million patient records exposed. This is an increase from the 905 medical data breaches that Protenus compiled in 2021.[18]

125. 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.[19]

---

[17] *9 reasons why healthcare is the biggest target for cyberattacks*, SwivelSecure, https://swivelsecure.com/solutions/ healthcare/healthcare-is-the-biggest-target-for-cyberattacks/ (last accessed May 30, 2024).

[18] *2022 Breach Barometer*, Protenus (2022), available at https://www.protenus.com/breach-barometer-report.

[19] 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.

126. Healthcare related breaches, in particular, have continued to rapidly increase because electronic patient data is seen as a valuable asset. In fact, entities that store patient information "have emerged as a primary target because they sit on a gold mine of sensitive personally identifiable information for thousands of patients at any given time. From social security and insurance policies, to next of kin and credit cards, no other organization, including credit bureaus, have so much monetizable information stored in their data centers."[20]

127. 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.[21]

128. Personal Information is a valuable property right.[22] The value of Personal Information as a commodity is measurable.[23] "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."[24] American companies are estimated to have spent

[20] Inside Digital Health, *How to Safeguard Hospital Data from Email Spoofing Attacks*, April 4, 2019, https://www.chiefhealthcareexecutive.com/view/how-to-safeguard-hospital-data-from-email-spoofing-attacks (last visited on May 21, 2024).

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

[22] *See* Marc van Lieshout, *The Value of Personal Data*, 457 IFIP Advances in Information and Communication Technology (May 2015), available at 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...").

[23] *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.

[24] *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.

over $19 billion on acquiring personal data of consumers in 2018.[25] 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.

129. As a result of its real value and the recent large-scale data breaches, identity thieves and cybercriminals have openly posted credit card numbers, SSNs, 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.

130. PHI is particularly valuable and has been referred to as a "treasure trove for criminals."[26] A cybercriminal who steals a person's PHI can end up with as many as "seven to 10 personal identifying characteristics of an individual."[27] 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.[28]

131. Personal information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[29] Experian reports that a stolen credit or debit card

---

[25] *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/.

[26] *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.").

[27] *Id.*

[28] 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.

[29] 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/.

number can sell for $5 to $110 on the dark web.[30] All-inclusive health insurance dossiers containing sensitive health insurance information, names, addresses, telephone numbers, email addresses, SSNs, and bank account information, complete with account and routing numbers, can fetch up to $1,200 to $1,300 each on the black market.[31] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[32] 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 SSN or credit card number.[33]

132. Criminals can use stolen Personal Information to extort a financial payment by "leveraging details specific to a disease or terminal illness."[34] 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."[35]

133. 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

[30] 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/.
[31] 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.
[32] *In the Dark*, VPNOverview.com, https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last accessed May 21, 2024).
[33] *See Health Care Systems and Medical Devices at Risk for Increased Cyber Intrusions for Financial Gain*, FBI Cyber Division (Apr. 8, 2014), https://nsarchive.gwu.edu/document/18867-national-security-archive-department-justice.
[34] *See* note 26, *supra*.
[35] *Id.*

willing to pay a premium to purchase from privacy protective websites."[36]

134. 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.

135. Indeed, cyberattacks against the healthcare industry have been common for over ten years with the 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."[37]

136. 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.[38]

137. In fact, according to the cybersecurity firm Mimecast, 90% of healthcare organizations experienced cyberattacks in the past year.[39]

138. Azura was on notice that the FBI has recently been concerned about data security

---

[36] 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.

[37] 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.

[38] 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.

[39] *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.

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)."[40]

139. 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.[41]

140. 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 Plaintiffs and class members.

141. 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.

142. 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

---

[40] Jim Finkle, *FBI Warns Healthcare Firms that they are Targeted by Hackers*, Reuters (Aug. 2014), https://www.reuters.com/article/us-cybersecurity-healthcare-fbi/fbi-warns-healthcare-firms-they-are-targeted-by-hackers-idUSKBN0GK24U20140820 (last accessed May 21, 2024).
[41] 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.

personal information. In announcing the fines, 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."[42]

143. Additionally, as companies became more dependent on computer systems to run their business,[43] e.g., working remotely as a result of the COVID-19 pandemic, and the Internet of Things ("IoT"), the danger posed by cybercriminals is magnified, thereby highlighting the need for adequate administrative, physical, and technical safeguards.[44]

144. Defendant was, or should have been, fully aware of the unique type and the significant volume of data on Azura's server(s), amounting to potentially hundreds of thousands of individuals' detailed Personal Information, and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

145. 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.

146. The injuries to Plaintiffs and class members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for the Personal Information of Plaintiffs and class members.

147. The ramifications of Azura's failure to keep secure the Personal Information of

---

[42] *Stolen Laptops Lead to Important HIPAA Settlements*, U.S. Department of Health and Human Services, (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.

[43] *Implications of Cyber Risk for Financial Stability*, Board of Governors of the Federal Reserve System, (May 12, 2022), https://www.federalreserve.gov/econres/notes/feds-notes/implications-of-cyber-risk-for-financial-stability-20220512.html.

[44] *Key Threats and Cyber Risks Facing Financial Services and Banking Firms in 2022*, Picus Security, (March 24, 2022), https://www.picussecurity.com/key-threats-and-cyber-risks-facing-financial-services-and-banking-firms-in-2022.

Plaintiffs and class members are long lasting and severe. Once Personal Information is stolen—particularly SSNs and PHI—fraudulent use of that information and damage to victims may continue for years.

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

148. 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.[45]

149. 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 SSN to obtain government benefits, or filing a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's SSN, rent a house, or receive medical services in the victim's name, and may even give the victim's personal information to police during an arrest, resulting in an arrest warrant being issued in the victim's name.[46] These criminal activities have and will result in devastating financial and personal losses to Plaintiffs and class members.

150. Because a person's identity is akin to a puzzle with multiple data points, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity—or track the victim to attempt other hacking crimes against the individual to obtain more data to perfect a crime.

---

[45] *See What to Know About Identity Theft*, Federal Trade Commission Consumer Advice (April 2021) https://www.consumer.ftc.gov/articles/what-know-about-identity-theft (last accessed on May 21, 2024).

[46] *See Warning Signs of Identity Theft*, Federal Trade Commission, https://www.identitytheft.gov/Warning-Signs-of-Identity-Theft (last visited May 30, 2024).

151. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or SSN. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate and trick individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails. Data Breaches can be the starting point for these additional targeted attacks on the victim.

152. One such example of criminals piecing together bits and pieces of compromised Personal Information for profit is the development of "Fullz" packages.[47] With "Fullz" packages, cyber-criminals can cross-reference two sources of Personal Information to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals.

153. The development of "Fullz" packages means here that the stolen Personal Information from the Data Breach can easily be used to link and identify it to Plaintiffs' and class members' phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not

[47] "Fullz" is jargon for data that includes the information of the victim, including, but not limited to, the name, address, credit card information, SSN, date of birth, and more. As a rule of thumb, the more information you have on a victim, the more money that can be made off of those credentials. Fullz are usually pricier than standard credit card credentials, commanding up to $100 per record (or more) on the dark web. Fullz can be cashed out (turning credentials into money) in various ways, including performing bank transactions over the phone with the required authentication details in hand. Even "dead Fullz," which are Fullz credentials associated with credit cards that are no longer valid, can still be used for numerous purposes, including tax refund scams, ordering credit cards on behalf of the victim, or opening a "mule account" (an account that will accept a fraudulent money transfer from a compromised account) without the victim's knowledge. *See*, *e.g.*, Brian Krebs, *Medical Records for Sale in Underground Stolen From Texas Life Insurance Firm*, Krebs on Security (Sep. 18, 2014), https://krebsonsecurity.com/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-firm/.

be included in the Personal Information that was accessed in the Data Breach, criminals may still easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over.

154. The existence and prevalence of "Fullz" packages means that the Personal Information stolen as a direct result of the Data Breach can easily be linked to the unregulated data (like driver's license numbers) of Plaintiffs and the other class members.

155. Thus, even if certain information (such as driver's license numbers) was not stolen in the Data Breach, criminals can still easily create a comprehensive "Fullz" package.

156. Then, this comprehensive dossier can be sold—and then resold in perpetuity—to crooked operators and other criminals (like illegal and scam telemarketers).

157. 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.

158. 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.[48]

159. 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.

---

[48] *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 (June 2007), https://www.gao.gov/assets/gao-07-737.pdf.

160. 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.[49]

161. 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.[50]

162. Theft of SSN 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 of his or her SSN, and a new identification number will not be provided until after the victim has suffered the harm. In other words, preventative action to defend against the possibility of misuse of a SSN is not permitted.

163. Even then, a new SSN may not be effective, as "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[51]

164. Due to the highly sensitive nature of SSNs, theft of SSNs 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

[49] Ari Lazarus, *How fast will identity thieves use stolen info?*, Military Consumer (May 24, 2017), https://www.militaryconsumer.gov/blog/how-fast-will-identity-thieves-use-stolen-info.
[50] *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/.
[51] Brian Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft.

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."[52]

165. This data, as one would expect, 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."[53]

166. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach because, there, victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change—names, PHI, and SSNs.

167. 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.[54] "Medical identity theft is a growing and dangerous crime that leaves its victims with little to no recourse for recovery," reported Pam Dixon, executive director of World Privacy Forum. "Victims often experience financial repercussions and worse yet, they frequently discover erroneous

[52] 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/.
[53] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, Network World (Feb. 6, 2015), https://www.networkworld.com/article/935334/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html.
[54] Michael Ollove, *The Rise of Medical Identity Theft in Healthcare*, KFF Health News (Feb. 7, 2014), https://kffhealthnews.org/news/rise-of-indentity-theft/.

information has been added to their personal medical files due to the thief's activities."[55]

168. 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."[56] It "is also more difficult to detect, taking almost twice as long as normal identity theft."[57] 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." [58] 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."[59]

169. 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:

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

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

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

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

---

[55] *Id.*
[56] 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/.
[57] *See* note 33, *supra*.
[58] *See* note 45, *supra*.
[59] *Id.*

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

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

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

h. Sales of medical debt arising from identity theft can perpetuate a victim's debt collection and credit problems, through no fault of their own.[60]

170. 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 that his or her SSN 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.

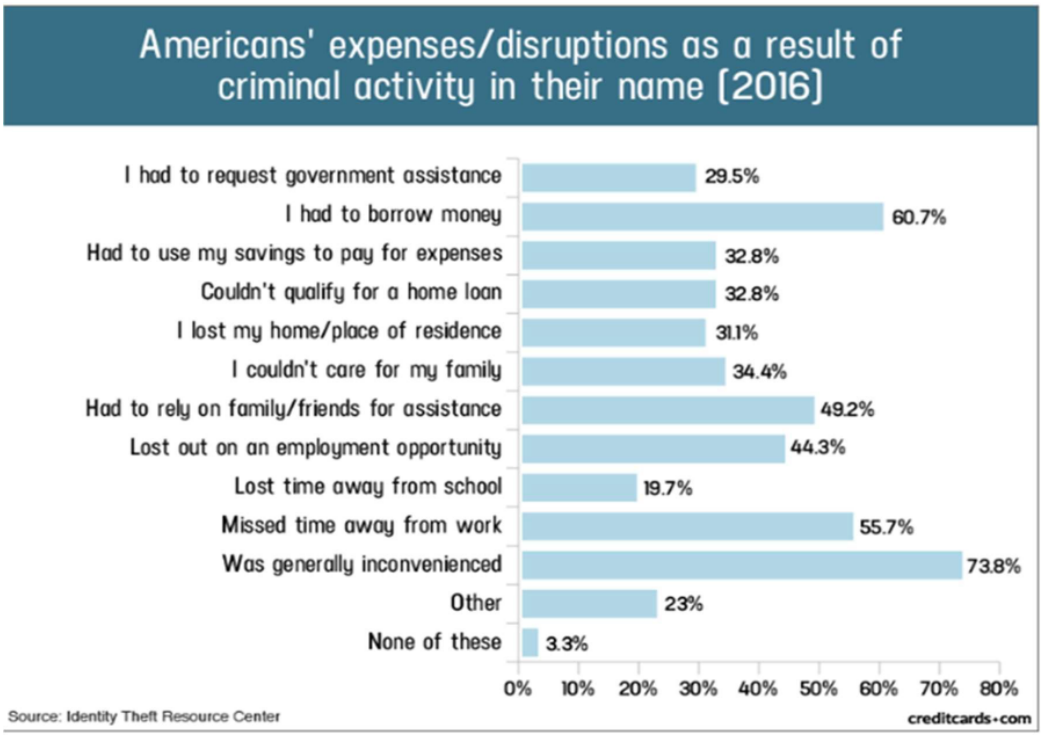
171. For example, on average it takes approximately three months for consumers to discover their identity has been stolen and used, and it takes some individuals up to three years to

[60] *See* note 55, *supra*.

learn that information.[61]

172. It is within this context that Plaintiffs 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.

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



174. Victims of the Data Breach, like Plaintiffs 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.[62]

[61] 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.

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

175. As a direct and proximate result of the Data Breach, Plaintiffs and class members have been placed at an imminent, immediate, and continuing increased risk of harm from fraud and identity theft. Plaintiffs 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 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.

176. Plaintiffs 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 Personal 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 Azura'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 Personal Information; and

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

177. Moreover, Plaintiffs 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 Plaintiffs' and class members' Personal Information.

178. 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, Azura knew or should have known about these dangers and strengthened its data security accordingly. Azura 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

179. Data disclosures and data breaches are preventable.[63] As Lucy Thompson wrote in

[63] Lucy L. Thompson, *Despite the Alarming Trends, Data Breaches Are Preventable*, Data Breach and Encryption Handbook (Lucy Thompson, ed., 2012).

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."[64] 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 . . . ."[65]

180. "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*."[66]

181. 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."[67]

182. Plaintiffs and class members entrusted their Personal Information to Azura as a condition of receiving healthcare-related services. Plaintiffs 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. Plaintiffs' and Class Members' Damages

183. To date, Azura has done nothing to provide Plaintiffs 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.

---

[64] *Id.* at 17.
[65] *Id.* at 28.
[66] *Id.* (emphasis added).
[67] *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 May 30, 2024).

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.

184. Plaintiffs and class members have been damaged by the compromise of their Personal Information in the Data Breach.

185. As a direct and proximate result of Azura's conduct, Plaintiffs and class members have been placed at an imminent, immediate, and continuing increased risk of harm from fraud and identity theft. Plaintiffs 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.

186. Plaintiffs 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 Plaintiffs and class members.

187. Plaintiffs 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.

188. Plaintiffs 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 SSNs, medical insurance accounts, bank accounts, and credit reports for unauthorized activity for years to come.

189. Defendant entirely failed to provide any compensation for the unauthorized release and disclosure of Plaintiffs and class members' Personal Information.

190. The retail cost of credit monitoring and identity theft monitoring can cost around $200 a year per class member. This is a reasonable and necessary cost to monitor to protect class members from the risk of identity theft that arose from Azura's Data Breach. This is a future cost for a minimum of five years that Plaintiffs and class members would not need to bear but for Azura's failure to safeguard their Personal Information.

191. Plaintiffs 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 Plaintiffs 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.

192. Further, as a result of Defendant's conduct, Plaintiffs 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.

193. As a direct and proximate result of Azura's actions and inactions, Plaintiffs and class members have suffered a loss of privacy and are at a present, imminent, and increased risk of future harm.

194. Moreover, Plaintiffs and class members have an interest in ensuring that their Personal Information, which is believed to remain in the possession of Azura, 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.

195. Many failures laid the groundwork for the occurrence of the Data Breach, starting with Azura's failure to incur the costs necessary to implement adequate and reasonable cybersecurity training, procedures, and protocols that were necessary to protect Plaintiffs' and class members' Personal Information.

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

197. Azura knew, or reasonably should have known, of the importance of safeguarding Personal Information and of the foreseeable consequences that would result if Plaintiffs' and class members' Personal Information was stolen, including the significant costs that would be placed on Plaintiffs and class members as a result of the breach.

198. The risk of improper disclosure of Plaintiffs' and class members' Personal Information was a known risk to Azura, and thus Azura was on notice that failing to take necessary steps to secure Plaintiffs' and class members' Personal Information from that risk left the Personal Information in a dangerous condition.

199. Azura disregarded the rights of Plaintiffs 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 Plaintiffs' 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 Plaintiffs and class members prompt and accurate notice of the Data Breach.

CLASS ALLEGATIONS

200. Plaintiffs bring 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 Fresenius Vascular Care, Inc. d/b/a Azura Vascular Care, including all who were sent notice of the Data Breach.

201. Alternatively, or in addition to the nationwide class, Plaintiffs seek to represent the following state classes:

Pennsylvania Class

All persons in the Commonwealth of Pennsylvania whose Personal Information was compromised in the Data Breach disclosed by Fresenius Vascular Care, Inc. d/b/a Azura Vascular Care, including all who were sent notice of the Data Breach.

Illinois Class

All persons in the state of Illinois whose Personal Information was compromised in the Data Breach disclosed by Fresenius Vascular Care, Inc. d/b/a Azura Vascular Care, including all who were sent notice of the Data Breach.

Maryland Class

All persons in the state of Maryland whose Personal Information was compromised in the Data Breach disclosed by Fresenius Vascular Care, Inc. d/b/a Azura Vascular Care, including all who were sent notice of the Data Breach.

202. Excluded from the class(es) are Defendant and its affiliates, parents, subsidiaries, officers, agents, and directors, and any entity in which Defendant has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; and any and all federal, state, or local governments; and the judge(s) presiding over this matter and the clerks and family members of said judge(s).

203. Plaintiffs reserve the right to modify or amend the definition of the proposed classes before the Court determines whether certification is appropriate.

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

205. **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, according to Defendant's disclosures, approximately 348,000 individuals' Personal Information was exposed in the Data Breach. The class members are identifiable within Defendant's records inasmuch as Defendant has already provided them with notification of the breach.

206. **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 Plaintiffs' and class members' PII/PHI from unauthorized access and disclosure;

b. Whether the computer systems and data security practices employed by Azura to protect Plaintiffs' 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. When Azura actually learned of the Data Breach;

d. 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 Plaintiffs and class members;

e. Whether Plaintiffs and class members suffered injury as a proximate result of Azura's negligent actions or failures to act;

f. Whether Azura failed to exercise reasonable care to secure and safeguard Plaintiffs' and class members' Personal Information;

g. Whether Azura adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

h. Whether an implied contract existed between class members and Azura, providing that Azura would implement and maintain reasonable security measures to protect and secure Plaintiffs' and class members' Personal Information from unauthorized access and disclosure;

i. Whether injunctive relief is appropriate and, if so, what injunctive relief is necessary to redress the imminent and currently ongoing harm faced by Plaintiffs and class members;

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

k. Whether Azura breached its duties to protect Plaintiffs' and class members' Personal Information; and

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

207. Azura engaged in a common course of conduct, giving rise to the legal rights sought to be enforced by Plaintiffs 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.

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

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

210. **Superiority**: A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. The damages and other financial detriment suffered by Plaintiffs and all other class members are relatively small compared to the burden and expense that would be required to individually litigate their claims against 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.

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

212. The litigation of the claims brought herein is manageable. Azura's uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of class members

demonstrate that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

213. Adequate notice can be given to class members directly using information maintained in Defendant's records.

214. Unless a class-wide injunction is issued, Azura may continue in its failure to properly secure the Personal Information of class members, Azura may continue to refuse to provide proper notification to class members regarding the Data Breach, and Azura may continue to act unlawfully as set forth in this complaint.

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

COUNT I
NEGLIGENCE
(On behalf of Plaintiffs and all Classes)

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

217. Azura collected the Personal Information of Plaintiffs and class members in the ordinary course of providing services and/or employment to Plaintiffs and class members.

218. Azura owed a duty to Plaintiffs and all other class members to exercise reasonable care in safeguarding and protecting their Personal Information in its possession, custody, or control. Azura's duty included a responsibility to implement processes by which it could detect a breach of its security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a data breach.

219. Azura knew, or should have known, the risks of collecting and storing Plaintiffs'

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.

220. 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.

221. Azura breached these duties by failing to exercise reasonable care in safeguarding and protecting Plaintiffs' 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 Plaintiffs' and class members' Personal Information.

222. It was reasonably foreseeable to Azura that its failure to exercise reasonable care in safeguarding and protecting Plaintiffs' 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 Plaintiffs' and class members' Personal Information to unauthorized individuals.

223. Azura's duty of care to use reasonable security measures also arose as a result of the special relationship that existed between Azura and patients. Azura was in a superior position to ensure that their systems were sufficient to protect against the foreseeable risk of harm to Plaintiffs and class members from a data breach.

224. Azura's duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Azura is bound by industry standards to protect confidential Personal Information.

225. But for Azura's negligent conduct or breach of the above-described duties owed to Plaintiffs and class members, their Personal Information would not have been compromised.

226. As a result of Azura's above-described wrongful actions, inaction, and want of ordinary care that directly and proximately caused the Data Breach, Plaintiffs and all other class members have suffered, and will continue to suffer, economic damages and other injury and actual harm in the form of, *inter alia*: (i) a substantially increased risk of identity theft and medical theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (ii) 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 (vii) actual or attempted fraud.

227. Plaintiffs and class members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

228. Plaintiffs and class members are also entitled to injunctive relief requiring Azura to, e.g., (i) strengthen their data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) continue to provide adequate credit monitoring to all class members.

COUNT II
NEGLIGENCE PER SE
(On behalf of Plaintiffs and all Classes)

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

230. 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").

231. 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 Personal Information.

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

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

234. Azura violated HIPAA Privacy and Security Rules and Section 5 of the FTCA by failing to use reasonable measures to protect Plaintiffs' 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 Plaintiffs and the other class members.

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

236. Plaintiffs 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.

237. 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.

238. It was reasonably foreseeable to Azura that its failure to exercise reasonable care in safeguarding and protecting Plaintiffs' 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 Plaintiffs' and class members' Personal Information to unauthorized individuals.

239. The injury and harm that Plaintiffs and 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. Plaintiffs and class members have suffered (and will continue to suffer) economic damages and other injury and actual harm in the form of, *inter alia*: (i) a substantially increased risk of identity theft and medical theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (ii) improper disclosure of their 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.

240. As a direct and proximate result of Azura's negligent conduct, Plaintiffs and class members have suffered injury and are entitled to compensatory, consequential, and punitive damages in an amount to be proven at trial.

COUNT III
BREACH OF FIDUCIARY DUTY
(On behalf of Plaintiffs and all Classes)

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

242. Plaintiffs and class members either directly or indirectly gave Azura their Personal Information in confidence, believing that Azura would protect that information. Plaintiffs 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 Plaintiffs' and class members' Personal Information created a fiduciary relationship between Azura and Plaintiffs 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 Plaintiffs' and class members' Personal Information.

243. Azura accepted and used Plaintiffs' and class members' Personal Information for its own pecuniary benefit and accepted the Personal Information with full knowledge of the need to maintain it as confidential, the need to implement appropriate data security measures, and the significant harm that would result to Plaintiffs and class members if the confidentiality of their Personal Information was breached.

244. Azura as their healthcare provider was in a superior position of trust and authority

to Plaintiffs and class members.

245. Plaintiffs and class members had no way to ensure that Azura's data security measures were adequate and no way to influence or verify the integrity of Azura's data security posture.

246. Azura has a fiduciary duty to act for the benefit of Plaintiffs and class members upon matters within the scope of their relationship. It breached that duty by failing to properly protect the integrity of the system containing Plaintiffs' 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 Plaintiffs and class members it collected. Azura also breached its fiduciary duty by failing to diligently discover, investigate, and give notice of the Data Breach in a reasonable and practicable period.

247. As a direct and proximate result of Azura's breaches of its fiduciary duties, Plaintiffs 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; (viii) future costs in terms of time, effort, and money that will be expended as result of the Data Breach for the remainder of the lives of Plaintiffs and class members; and (ix) the diminished value of Azura's services they received.

COUNT IV
BREACH OF IMPLIED CONTRACT
(On behalf of Plaintiffs and all Classes)

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

249. Azura required Plaintiffs and class members to provide, or authorize the transfer of, their Personal Information in order for Azura to provide services. In exchange, Azura entered into implied contracts with Plaintiffs and class members in which Azura agreed to comply with its statutory and common law duties to protect Plaintiffs' and class members' Personal Information and to timely notify them in the event of a data breach.

250. The implied promise of confidentiality includes consideration beyond those pre-existing general duties owed under HIPAA or other state of federal regulations. The additional consideration included implied promises to take adequate steps to comply with specific industry data security standards and FTC guidelines on data security.

251. The implied promises include but are not limited to: (1) taking steps to ensure that any agents who are granted access to Personal Information also protect the confidentiality of that data; (2) taking steps to ensure that the information that is placed in the control of its agents is restricted and limited to achieve an authorized medical purpose; (3) restricting access to qualified and trained agents; (4) designing and implementing appropriate retention policies to protect the information against criminal data breaches; (5) applying or requiring proper encryption; (6) implementing multifactor authentication for access; and (7) taking other steps to protect against foreseeable data breaches.

252. Plaintiffs and class members would not have provided their Personal Information to Azura, or would not have agreed to have that information provided to Azura, had they known

that Azura would not safeguard their Personal Information, as promised, or provide timely notice of a data breach.

253. Azura recognized that Plaintiffs' and class member's Personal Information is highly sensitive and must be protected, and that this protection was of material importance as part of the bargain to Plaintiffs and the other class members.

254. Plaintiffs and class members fully performed their obligations under their implied contracts with Azura.

255. Azura breached the implied contracts by failing to safeguard Plaintiffs' and class members' Personal Information and by failing to provide them with timely and accurate notice of the Data Breach.

256. The losses and damages Plaintiffs and class members sustained (as described above) were the direct and proximate result of Azura's breach of its implied contracts with Plaintiffs and class members.

257. As a direct and proximate result of Azura's conduct, Plaintiffs and class members suffered and will continue to suffer damages in an amount to be proven at trial.

COUNT V
BREACH OF CONFIDENCE
(On behalf of Plaintiffs and all Classes)

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

259. Plaintiffs 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.

260. As a healthcare provider, Azura has a special relationship to its patients and other

affiliated persons, such as Plaintiffs and the class members.

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

262. 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.

263. Azura owed a duty to Plaintiffs 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.

264. Azura had an obligation to maintain the confidentiality of Plaintiffs' and the class members' Personal Information.

265. Plaintiffs 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.

266. As a result of the parties' relationship, Azura had possession and knowledge of the confidential Personal Information and confidential medical records of Plaintiffs and the class.

267. Plaintiffs' and class members' Personal Information is not generally known to the public and is confidential by nature.

268. Plaintiffs and class members did not consent to nor authorize Azura to release or disclose their Personal Information to an unknown threat actor.

269. Azura breached the duties of confidence it owed to Plaintiffs and the class when Plaintiffs' and class members' Personal Information was disclosed to unknown criminal hackers.

270. 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 PII/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 Plaintiffs' and class members' Personal Information, inclusive of medical records/information, to a criminal third party.

271. But for Azura's wrongful breach of its duty of confidences owed to Plaintiffs and the class members, their privacy, confidences, and Personal Information would not have been compromised.

272. As a direct and proximate result of Azura's breach of confidences, Plaintiffs 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 Plaintiffs and the class as patients;

b. Loss of the privacy and confidential nature of their Personal Information;

c. Theft of their Personal Information;

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 Personal Information being placed in the hands of criminals;

i. Damages to and diminution in value of their Personal Information 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 Personal Information, 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 Plaintiffs' 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 Personal Information.

273. Additionally, Azura received payments from Plaintiffs and class members for services with the understanding that Azura would uphold its responsibilities to maintain the confidences of Plaintiffs' and class members' Personal Information.

274. Azura breached the confidence of Plaintiffs 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 Plaintiffs' and class members' expense.

275. As a direct and proximate result of Azura's breach of its duty, Plaintiffs 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 VI
VIOLATION OF THE ILLINOIS CONSUMER FRAUD AND DECEPTIVE BUSINESS PRACTICES ACT ("CFA"), 815 Ill. Comp. Stat. §§505/1, *et seq.*
(On Behalf of Plaintiff Banks and the Illinois Class)

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

277. Plaintiff Banks and the Illinois Class are "consumers" as defined in 815 Ill. Comp. Stat. § 505/1(e). Plaintiff Banks, the Illinois Class, and Defendant are "persons" as defined in 815 Ill. Comp. Stat. § 505/1(c).

278. Defendant is engaged in "trade" or "commerce," including the provision of

services, as defined under 815 Ill. Comp. Stat. § 505/1(f). Defendant engages in the sale of "merchandise" (including "services" as defined by 815 Ill. Comp. Stat. § 505/1(b) and (d)).

279. Defendant engaged in deceptive and unfair acts and practices, misrepresentation, and the concealment and omission of material facts in connection with the sale and advertisement of their services in violation of the CFA, including: (1) failing to maintain adequate data security to keep Plaintiff Banks' and the Illinois Class's sensitive Private Information from being stolen by cybercriminals and failing to comply with applicable state and federal laws and industry standards pertaining to data security, including HIPAA and the FTC act; (2) failing to disclose or omitting material facts to Plaintiff Banks and the Illinois Class regarding its lack of adequate data security and inability or unwillingness to properly secure and protect the Private Information of Plaintiff Banks and the Illinois Class; (3) failing to disclosure or omitting material facts to Plaintiff Banks and the Illinois Class about Defendant's failure to comply with the requirements of relevant federal and state laws pertaining to the priacy and security of the Private Information of Plaintiff Banks and the Illinois Class; and (4) failing to take proper action following the Data Breach to enact adequate privacy and security measures and protect Plaintiff Banks and the Illinois Class's Private Information and other personal information from further unauthirzed disclosure, release, data breaches, and theft.

280. These actions also constitute deceptive and unfair acts or practices because Defendant knew the facts about its inadequate data security and failure to comply with applicable state and federal laws and industry standards would be unknown to and not easily discoverable by Plaintiff Banks and the Illinois Class and defeat their reasonable expectations about the security of their PII and PHI.

281. Defendant intended that Plaintiff Banks and the Illinois Class rely on its deceptive

and unfair acts and practices and the concealment and omission of material facts in connection with Defendant's offering of goods and services.

282. Defendant's wrongful practices were and are injurious to the public because those practices were part of Defendant's generalized course of conduct that applied to the Illinois Class. Plaintiff Banks and the Illinois Class have been adversely affected by Defendant's conduct and the public was and is at risk as a result thereof.

283. Defendant also violated 815 ILCS 505/2 by failing to immediately notify Plaintiff Banks and the Illinois Class of the nature and extent of the Data Breach pursuant to the Illinois Personal Information Protection Act, 815 ILCS 530/1, *et seq*.

284. As a result of Defendant's wrongful conduct, Plaintiff Banks and the Illinois Class were injured in that they never would have provided their PII and PHI to Defendant, or paid for Defendant's services, had they known or been told that Defendant failed to maintain sufficient security to keep their PII and PHI from being hacked and taken and misused by others.

285. As a direct and proximate result of Defendant's violations of the CFA, Plaintiff Banks and the Illinois Class have suffered harm, including actual instances of identity theft; loss of time and money resolving fraudulent charges; loss of time and money obtaining protections against future identity theft; financial losses related to the payments or services made to Defendant that Plaintiff Banks and the Illinois Class would not have made had they known of Defendant's inadequate data security; lost control over the value of their PII and PHI; unreimbursed losses relating to fraudulent charges; harm resulting from damaged credit scores and information; and other harm resulting from the unauthorized use or threat of unauthorized use of stolen PII and PHI, entitling them to damages in an amount to be proven at trial. Specifically, Plaintiff Banks experienced fraudulent charges on his debit card and was required to obtain a new one. Plaintiff

Banks suffered economic injury because he was unable to make purchases with his debit card while he awaited the replacement card.

286. Pursuant to 815 Ill. Comp. Stat. § 505/10a(a), Plaintiff Banks and the Illinois Class seek actual and compensatory damages, injunctive relief, and court costs and attorneys' fees as a result of Defendant's violations of the CFA.

COUNT VII
UNJUST ENRICHMENT
(On behalf of Plaintiffs and all Classes)

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

288. This claim is pleaded in the alternative to Plaintiffs' contract claim, pursuant to Fed. R. Civ. P. 8(d).

289. Plaintiffs and class members conferred a monetary benefit upon Azura in the form of monies paid for healthcare services or other services.

290. Azura accepted or had knowledge of the benefits conferred upon it by Plaintiffs and class members. Azura also benefitted from the receipt of Plaintiffs' and class members' Personal Information.

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

292. Under principles of equity and good conscience, Azura should not be permitted to retain the money belonging to Plaintiffs and class members because Azura failed to adequately

implement the data privacy and security procedures for itself that Plaintiffs and class members paid for and that were otherwise mandated by federal, state, and local laws, and industry standards.

293. Azura should be compelled to provide for the benefit of Plaintiffs and class members all unlawful proceeds received by it as a result of its misconduct and the Data Breach.

COUNT VIII
VIOLATIONS OF THE MARYLAND PERSONAL INFORMATION PROTECTION ACT
Md. Code Ann., Com. Law, §§13-301, *et seq*. ("MPIPA")
(On Behalf of the Plaintiff Welzenbach and the Maryland Class)

294. Plaintiffs incorporate all previous paragraphs as if fully set forth below.

295. This count is brought on behalf of Plaintiff Welzenbach and the Maryland Class. For purposes of this count, "Plaintiff" refers to Plaintiff Welzenbach.

296. Under the Maryland Personal Information Protection Act ("MPIPA"), Md. Code Ann., Com. Law, § 14-3503(a), "[t]o protect Personal Information from unauthorized access, use, modification, or disclosure, a business that owns or licenses Personal Information of an individual residing in the State shall implement and maintain reasonable security procedures and practices that are appropriate to the nature of Personal Information owned or licensed and the nature and size of the business and its operations."

297. Defendant is a business that owns or licenses computerized data that includes Personal Information as defined by Md. Code Ann., Com. Law, § 14-3501(b)(1).

298. Plaintiff and class members are "individuals" and "customers" as defined in Md. Code Ann., Com. Law, §§ 14-3502(a) and 14-3503.

299. Plaintiff and class members' Personal Information includes "[h]ealth information" and "[p]ersonal information" as covered under Md. Code Ann., Com. Law, §§ 14-3501(d)-(e).

300. Defendant did not maintain reasonable security procedures and practices

appropriate to the nature of the Personal Information owned or licensed and the nature and size of its business and operations in violation of Md. Code Ann., Com. Law, § 14-3503.

301. The Data Breach was a "breach of the security of a system" as defined by Md. Code Ann., Com. Law, § 14-3504(1).

302. Under Md. Code Ann., Com. Law, § 14-3504(b)(1), "[a] business that owns or licenses computerized data that includes Personal Information of an individual residing in the State, when it discovers or is notified of a breach of the security system, shall conduct in good faith a reasonable and prompt investigation to determine the likelihood that Personal Information of the individual has been or will be misused as a result of the breach."

303. Under Md. Code Ann., Com. Law, §§ 14-3504(b)(2) and 14-3504(c)(2), "[i]f, after the investigation is concluded, the business determines that the breach of the security of the system creates a likelihood that personal information has been or will be misused, the owner or licensee of the computerized data shall notify the individual of the breach" and that notification "shall be given as soon as reasonably practical but not later than 45 days after the business discovers or is notified of the breach of a security system."

304. Under Md. Code Ann., Com. Law §14-3504(c)(3) the notification the "business that is required to notify an owner or licensee of personal information of a breach of security of a system under paragraph (1) of this subsection shall share with the owner or licensee information relative to the breach."

305. Because Defendant discovered the security breach and had notice of the security breach, Defendant had an obligation to disclose the Data Breach in a timely fashion as mandated by Md. Code Ann., Com. Law, §§ 14-3504(b)(2) and 14-3504(c)(2).

306. Defendant failed to notify Plaintiff and class members that an unauthorized user(s)

breached their email system and was in possession of their Personal Information in a timely manner. By failing to disclose all of the information that was available to Defendant in a timely manner, Defendant violated Md. Code Ann., Com. Law, §§ 14-3504(b)(2) and 14-3504(c)(2).

307. As a direct and proximate result of Defendant's violations of Md. Code Ann., Com. Law, §§ 14-3504(b)(2) and 14-3504(c)(2), Plaintiff and class members have suffered and will continue to suffer damages.

308. Pursuant to Md. Code Ann., Com. Law, § 14-3508, Defendant's violations of Md. Code Ann., Com. Law, §§ 14-3504(b)(2) and 14-3504(c)(2) are unfair or deceptive trade practices within the meaning of the Maryland Consumer Protection Act (codified at Md. Code Ann., Com. Law, § 13-301 et seq.) and are subject to the enforcement and penalty provisions contained within the MCPA.

COUNT IX
DECLARATORY AND INJUNCTIVE RELIEF
(On behalf of Plaintiffs and all Classes)

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

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

311. Azura owes a duty of care to Plaintiffs and class members that require it to adequately secure Plaintiffs' and class members' Personal Information.

312. Azura still possesses the Personal Information of Plaintiffs and class members.

313. Azura has not satisfied its contractual obligations and legal duties to Plaintiffs and class members.

314. Actual harm has arisen in the wake of the Data Breach regarding Azura's

contractual obligations and duties of care to provide security measures to Plaintiffs and class members. Further, Plaintiffs and class members are at risk of additional or further harm due to the exposure of their Personal Information and Azura's failure to address the security failings that led to such exposure.

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

316. Plaintiffs, therefore, seek a declaration (1) that Azura'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, Azura must implement and maintain reasonable security measures, including, but not limited to, the following:

a. Prohibit Azura from engaging in the wrongful and unlawful acts described herein;

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

c. Requiring Azura to protect, including through encryption, all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state, or local laws;

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

e. Ordering that Azura audit, test, and train its security personnel and

employees regarding any new or modified data security policies and procedures;

f. Ordering that Azura purge, delete, and destroy, in a reasonably secure manner, any Personal Information not necessary for its provision of services;

g. Ordering that Azura conduct regular database scanning and security checks; and

h. Prohibiting Azura from maintaining Personal Information of Plaintiffs and class members on a cloud-based database;

i. Requiring Azura to segment data by, among other things, creating firewalls and access controls so that if one area of Azura's network is compromised, hackers cannot gain access to other portions of Azura's systems;

j. Ordering that Azura 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;

k. Requiring Azura to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceeding paragraphs, as well as randomly and periodically testing employees compliance with Azura's policies, programs, and systems for protecting personal identifying information;

l. Requiring Azura to meaningfully educate all class members about the

threats they face as a result of the loss of their confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves;

m. Requiring Azura to implement logging and monitoring programs sufficient to track traffic to and from Azura's servers; and for a period of 10 years, appointing a qualified and independent third-party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Azura's compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court's final judgment;

n. Such other and further relief as this Court may deem just and proper.

PRAYER FOR RELIEF

Plaintiffs, 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(es) as requested herein, designating Plaintiffs as class representatives, and appointing Plaintiffs' counsel as Class Counsel;

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

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

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

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

JURY TRIAL DEMANDED

Plaintiffs demand a trial by jury of all claims so triable.

Dated: May 30, 2024

Respectfully submitted,

/s/ Andrew W. Ferich

Andrew W. Ferich (ID No. 313696)
Chloe R. DeOnna (ID No. 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

Benjamin F. Johns (ID No. 201373)
Samantha E. Holbrook (ID No. 311829)
SHUB & JOHNS LLC
Four Tower Bridge
200 Barr Harbor Drive, Suite 400
Conshohocken, PA 19428
Telephone: (610) 477-8380
Facsimile: (856) 210-9088
bjohns@shublawyers.com
sholbrook@shublawyers.com

Interim Class Counsel for Plaintiffs

CERTIFICATE OF SERVICE

The undersigned hereby certifies that on this 30th day of May, 2024, a true and correct copy of the foregoing was filed with the Clerk of Court via the Court's CM/ECF system for electronic service on all counsel of record.

Dated: May 30, 2024

/s/Andrew Ferich
Andrew Ferich