Paul L. Stoller (No. 016773)
Lincoln Combs (No. 025080)
GALLAGHER & KENNEDY, P.A.
2575 E. Camelback Road, Suite 1100
Phoenix, Arizona 85016-9225
Telephone: (602) 530-8054
Facsimile: (602) 530-8500
paul.stoller@gknet.com
lincoln.combs@gknet.com

Andrew S. Friedman (005425)
William F. King (023941)
BONNETT FAIRBOURN FRIEDMAN & BALINT, P.C.
2325 E. Camelback Road #300
Phoenix, Arizona 85016
Telephone: (602) 274-1100
afriedman@bffb.com
bking@bffb.com

Interim Co-Lead Class Counsel

[Additional Counsel on Signature Page]

REDACTED

UNITED STATES DISTRICT COURT

DISTRICT OF ARIZONA

IN RE BANNER HEALTH DATA BREACH LITIGATION

Case No. 2:16-cv-02696-PHX-SRB

PLAINTIFFS' SECOND CONSOLIDATED AMENDED CLASS ACTION COMPLAINT

DEMAND FOR JURY TRIAL

TABLE OF CONTENTS

Pursuant to the stipulation of the parties [Doc. 108] and the Court's order [Doc. 109], Plaintiffs Howard Chen, Betty Clayton, Stacey Halpin, Kim Maryniak, Summer Sadira, and Stan Griep, on behalf of themselves and all others similarly situated, allege for their Second Consolidated Amended Class Action Complaint[1] as follows:

INTRODUCTION

1. Banner Health is one of the largest, nonprofit healthcare systems in the country, generating approximately $7 billion in annual revenue through health services and insurance plans in six states. Banner's business requires it to maintain millions of electronic health and insurance records, personal and professional information about its over 50,000 healthcare providers, and payment card information from customers of its food and beverage outlets at its facilities.

2. Healthcare and insurance companies have for years been on high alert due to the risk of a criminal cyber-attack. There have been a number of high profile data breaches in the industry and the FBI and others have warned companies they will continue to be targets because they maintain sensitive, personal information that is also highly valuable to cybercriminals. In particular, the combination of social security numbers, personally identifying information ("PII") (such as names, addresses, and birth dates), and protected health information ("PHI") including medical histories allows criminals to engage in identity theft as well as medical fraud which, for example, can cause a patient to receive a bill for medical treatment they never received or to be denied treatment because of inaccuracies in their records.

---

[1] Plaintiffs acknowledge this Court's December 20, 2017, order granting in part and denying in part Banner Health's Motion to Dismiss (the "Order") [Doc. 106], and in particular, the dismissal of Plaintiffs' claims for Breach of Contract (Third Cause of Action), Breach of Implied Covenant of Good Faith and Fair Dealing (Fourth Cause of Action), and Breach of the Implied Duty to Perform with Reasonable Care (Fifth Cause of Action) (collectively the "Dismissed Claims"). Plaintiffs have included the Dismissed Claims in this Second Consolidated Amended Class Action Complaint solely to preserve all rights on appeal. *See Taylor ex rel. Thomson v. Zurich Am. Ins. Co.*, CV11-08110-PCT-JAT, 2013 WL 1340014, at *8 (D. Ariz. Apr. 1, 2013). Banner need not answer or otherwise respond to those claims.

3. Banner could have prevented the data breach but for its failure to implement reasonable cybersecurity precautions, as required by both its own promises and the law. Banner promised patients and insurance plan members that it was both HIPAA compliant and "committed to protecting the confidentiality of [their] information." But Banner failed to take a number of fundamental, industry-standard steps to ensure adequate information security—and apparently did so to enhance its own bottom line profitability.

[redacted]

4. [redacted]

[redacted]

5. Banner nevertheless continued to neglect its information security. The law and industry standards required Banner to take precautions such as implementing multi-factor authentication, keeping key systems (including payment card information ("PCI") systems) behind firewalls, implementing access controls to limit access to sensitive data on a "need-to-know" basis, adequately encrypting sensitive data, logging and monitoring in compliance with cybersecurity standards, and segmenting its networks to prevent intruders from moving freely within the Banner environments. Banner failed at every one of these requirements and more.

6. In June 2016, hackers took advantage of Banner's many information security failings. [redacted] Moreover, although there was no legitimate reason for having its PCI system devices connected to databases that maintain patient, member, and provider PHI and PII, Banner had failed to segregate its systems and instead left the PCI server connected through its enterprise network to its most sensitive and important information—the PII and PHI of Plaintiffs and the Class Members. As a result of this utter lack of network segmentation, the hackers were next able to move laterally through Banner's enterprise network to access and copy the PHI and PII in those databases. The hackers' lateral movement through Banner's systems was rapid, with the hackers taking advantage of Banner's failure to implement network segmentation and access controls, among other things. Less than one week after first accessing Banner's network, the hackers accessed and copied large amounts of PII, PHI, and PCI. They then transmitted the data to a location outside Banner's network and securely deleted many of the files they had created in order to cover their tracks and obfuscate the extent of the breach. It was not until two weeks after the hackers first entered Banner's network that Banner suspected an infiltration, [redacted]

7. The hackers succeeded in obtaining names, addresses, dates of birth, social security numbers, provider information, medical histories, and more. In other words, they acquired all that is needed to engage in identity theft and medical fraud of nearly four million people. This is already happening. The cybercriminal group that Banner's forensic examiner identified as the culprit is known in the information security community as a [redacted] meaning their goal in acquiring PII, PHI, and PCI is to monetize it. It is therefore assured that the data they stole either has already or

will soon make it to criminals determined to engage in identity theft, medical fraud, and the like. The four million victims of the data breach thus face a variety of present, imminent, and long-lasting risks. Already, many have been victimized by fraud attempts—and they may be the fortunate ones because identity theft and medical fraud are often discovered, if at all, only after severe credit harm, false account charges or other damages have already occurred.

8. Plaintiffs are Banner patients, insurance plan members, plan beneficiaries, payment card users, and healthcare providers. Each of them received a letter approximately two months after Banner discovered the data breach, stating that the security of their personal information had been compromised. They now bring this action on behalf of themselves and all others similarly situated. They seek an injunction requiring Banner to reform its information security practices. And they seek the restitution, damages, and other monetary relief necessary to compensate them as well as to deter future misconduct of this type.

PARTIES

I. Plaintiffs

A. Howard Chen

9. Plaintiff Howard Chen is a citizen and resident of Arizona. Dr. Chen is a physician and surgeon, licensed as a Doctor of Medicine in Arizona and a Fellow at the American Board of Ophthalmology, and currently owns and operates a private practice in Goodyear, Arizona.

10. From March 2011 to the present, Dr. Chen has been on staff in the Department of Surgery at Banner Boswell Medical Center. From May 1, 2014, to the present, Dr. Chen has been on staff in the Departments of Surgery at Banner Thunderbird Medical Center. His appointment letters from the hospital each confirmed that he was covered by Banner's "Medical Staff Bylaws, Rules and Regulations, and Policies."

11. In addition to staff privileges, Dr. Chen entered into an employee provider contract with Banner Arizona Medical Clinic from December 1, 2010, to August 28, 2013, before starting his private practice.

12. Beginning in December 2010 until he started his private practice, Dr. Chen was also enrolled in the health and dental insurance plans operated by Banner and paid all premiums when due. Dr. Chen routinely received medical and dental care from physicians in the Banner network.

13. Banner demanded, collected, and received Dr. Chen's PII and PHI in connection with his employment, as a condition of receiving health and dental insurance, and as a prerequisite to receiving privileges at Thunderbird and Boswell hospitals. At all relevant times, Banner maintains Dr. Chen's PHI and PII in its data systems.

14. Dr. Chen was never warned about the deficiencies in Banner's information security systems. To the contrary, Dr. Chen routinely received information stating that data privacy was a serious concern at Banner and that everyone should work to maintain the security of all PHI and PII.

15. On or about August 3, 2016, Dr. Chen received correspondence from Banner informing him that his personal information may have been compromised as a result of the Banner breach. In the letter, Dr. Chen was offered one year of "credit and identity monitoring" through Kroll. On or about November 18, 2016, Dr. Chen enrolled in Kroll's monitoring service, but does not believe the company provides the coverage he needs following the breach. For example, Kroll's service does not monitor Dr. Chen's National Provider Identity ("NPI") number, IRS Tax Identification Number ("TIN"), or Drug Enforcement Agency ("DEA") number. Banner has asked physicians to monitor their own DEA numbers, and Kroll does nothing to monitor this vitally important PII that, if compromised, could adversely affect Dr. Chen's ability to practice medicine.

16. Dr. Chen has followed Banner's instructions and is monitoring his DEA number, as well as his TIN and NPI, which takes time away from his practice and ability to earn a living.

17. Dr. Chen now lives in fear of unauthorized misuse and exploitation of his confidential information, theft, and related financial fraud and resulting harm. Dr. Chen has spent and will spend time, including time away from his practice, and money safeguarding his personal and private information from this cyber-attack, mindful that his information continues to remain at high risk for fraud, including continuing identity theft, and the continuing risk of being victimized by reason of Banner's conduct.

B. Betty Clayton

18. Plaintiff Betty Clayton is a citizen and resident of the state of Arizona.

19. Ms. Clayton was a patient at Banner Good Samaritan Medical Center, a Banner facility in Phoenix, Arizona. As a condition of receiving treatment, Banner demanded, collected, and received Ms. Clayton's PII and PHI, which Banner maintained in its data systems.

20. At the time of admission, Banner entered into a "Banner Health Financial Agreement" and a "Medical Treatment Agreement (Conditions of Admission)" with Ms. Clayton.

21. Ms. Clayton's PII and PHI were collected pursuant to and under the terms of those agreements.

22. On or about August 8, 2016, Ms. Clayton learned through news accounts about the breach, and called the 1-855 telephone number posted on Banner's website. She was informed by the Banner representative on the hotline that her PII and PHI was among the information accessed and stolen by the cyber attackers and that she was affected by the breach. Shortly after that conversation she received a letter from Banner confirming that she had been a victim of Banner's data breach.

23. To her knowledge, Ms. Clayton is not yet the victim of identity theft. However, she has suffered substantial, irreparable harm by virtue of the fact that her PII and PHI was compromised and disclosed to one or more criminals whose identity remains unknown, and that her PII and PHI will remain at risk, in the public domain, permanently.

24. Plaintiff Betty Clayton faces imminent risk of harm as a result of the breach.

25. Ms. Clayton now lives in fear of further unauthorized misuse and exploitation of her confidential information, theft, and related financial fraud and resulting harm. Ms. Clayton has spent and will spend time and money safeguarding her personal and private information from this cyber-attack, mindful that her information continues to remain at high risk for fraud, including continuing identity theft, and the continuing risk of being victimized by reason of Banner's conduct.

C. Stacey Halpin

26. Plaintiff Stacey Halpin is a citizen and resident of the state of Arizona.

27. In 2009 and 2011, Ms. Halpin was a patient at Banner Desert Medical Center located in Mesa, Arizona. In 2016, Ms. Halpin was a patient at Banner Baywood Medical Center also located in Mesa, Arizona.

28. As a condition of receiving care, Banner demanded, collected, and received Ms. Halpin's PII and PHI as a prerequisite to receiving care. Banner maintained this information in its data systems.

29. Ms. Halpin was also formerly employed as a radiology technician at Banner Desert Medical Center from approximately 2007 to 2011. As a part of her employment, Ms. Halpin entered into an employee contract with Banner. Pursuant to that contract, Banner demanded, collected, and received Ms. Halpin's PII, which Banner maintained in its data systems.

30. From 2007 to 2013, Ms. Halpin was enrolled in a Banner health insurance plan, and paid premiums on a regular basis. As a result, Banner demanded, collected and received Ms. Halpin's PII and PHI, which Banner maintained in its data systems.

31. Finally, during her stays as a patient at Banner Baywood, Ms. Halpin's family purchased food and beverages at the facility's cafeteria using the family credit card. As part of that transaction, Banner collected and received Ms. Halpin's PCI, which Banner maintained in its data systems.

32. On or about August 3, 2016, Ms. Halpin, her husband, and her son received a letter from Banner informing her that her PII and PHI may have been compromised as a

result of the data breach. After receiving the letter, Ms. Halpin enrolled in the one-year credit monitoring service offered through Kroll.

33. As a result of the breach, two bank accounts were falsely opened in her name. One account was opened with Citibank, and the other with Sioux Falls. Kroll did not identify the Citibank account as potentially fraudulent even though she was participating in Kroll's credit monitoring service when the account was opened.

34. Additionally, when Ms. Halpin attempted to file her income taxes in February 2017 for the taxable year 2016, she was unable to do so. An unknown, unauthorized person already filed taxes using her PII taken in the Banner data breach. Remedying this situation will take a significant amount of Ms. Halpin's time, and will require her to spend additional time and money in order to restore identity.

35. Ms. Halpin now lives in fear of further unauthorized misuse and exploitation of her confidential information, theft, and related financial fraud and resulting harm.

36. Ms. Halpin has spent and will spend time and money safeguarding her personal and private information from this cyber-attack, mindful that her information continues to remain at high risk for fraud, including continuing identity theft, and the continuing risk of being victimized by reason of Banner's conduct.

D. Kim Maryniak

37. Plaintiff Kim Maryniak is a citizen and resident of the state of Arizona.

38. Ms. Maryniak is currently employed as the Director of Professional Practice at Banner Thunderbird Medical Center, a Banner facility, and has worked there since 2015. As a part of her employment, Ms. Maryniak had an employee contract with Banner. Pursuant to that contract, Banner demanded, collected, and received Ms. Maryniak's PII, which Banner maintained in its data systems.

39. As part of her employment, Ms. Maryniak was enrolled in Banner's health and dental insurance plans, and paid premiums on a regular basis. As a result, Banner demanded, collected, and received Ms. Maryniak's PII and PHI, which Banner maintained in its data systems.

40. Ms. Maryniak was a patient at Banner Boswell Medical Center and Banner Del E. Webb Medical Center, Banner facilities located in Sun City, Arizona. Banner demanded, collected, and received Ms. Maryniak's PII and PHI while she was a patient, which Banner maintained in its data systems.

41. Finally, during her time at Banner Thunderbird, Ms. Maryniak purchased food and beverages at the facility's cafeteria using her personal credit card. As part of that transaction, Banner collected and received Ms. Maryniak's payment card information, which Banner maintained in its data systems.

42. On or about August 3, 2016, Ms. Maryniak and her family received letters from Banner informing her that her PII and PHI may have been compromised as a result of the data breach. Ms. Maryniak received two letters: one as an employee, and one as a former patient. After receiving the notifications, Ms. Maryniak enrolled in the one-year credit monitoring service offered through Kroll.

43. Following the breach, there were unauthorized attempts to use her credit card. Additionally, Ms. Maryniak's Verizon Communications and Google accounts were used or changed without her authorization.

44. Ms. Maryniak now lives in fear of further unauthorized misuse and exploitation of her confidential information, theft, and related financial fraud and resulting harm. Ms. Maryniak has spent and will spend time and money safeguarding her personal and private information from this cyber-attack, mindful that her information continues to remain at high risk for fraud, including continuing identity theft, and the continuing risk of being victimized by reason of Banner's conduct.

E. Summer Sadira

45. Plaintiff Summer Sadira is a citizen and resident of the state of Colorado.

46. Ms. Sadira was a patient at Banner Health Clinic, a Banner facility in Loveland, Colorado. As a condition of receiving treatment, Banner demanded, collected, and received Ms. Sadira's PII and PHI, which Banner maintained in its data systems.

47. During her stays as a patient at Banner Health Center, Ms. Sadira purchased food and beverages at the facility's cafeteria using her personal credit card. As part of that transaction, Banner collected and received Ms. Sadira's PCI, which Banner maintained in its data systems.

48. On or about August 3, 2016, Ms. Sadira received a letter from Banner informing her that her PII and PHI may have been compromised as a result of the data breach. Due to Ms. Sadira's enrollment in Colorado's Address Confidentiality Program, Ms. Sadira did not feel safe by providing Banner with additional information to register with Kroll credit monitoring. Due to the breach, Ms. Sadira's real address is in the public domain, thwarting the purpose of the Address Confidentiality Program, and potentially endangering her and her family.

49. To her knowledge, Ms. Sadira is not yet a victim of identity theft. However, she has suffered substantial, irreparable harm by virtue of the fact that her PII and PHI was compromised and disclosed to one or more criminals whose identity remains unknown, and that her PII and PHI will remain at risk, in the public domain, permanently.

50. Ms. Sadira now lives in fear of further unauthorized misuse and exploitation of her confidential information, theft, and related financial fraud and resulting harm. Ms. Sadira has spent and will spend time and money safeguarding her personal and private information from this cyber-attack, mindful that her information continues to remain at high risk for fraud, including continuing identity theft, and the continuing risk of being victimized by reason of Banner's conduct.

F. Stan Griep

51. Plaintiff Stan Griep is a citizen and resident of the state of Colorado.

52. Mr. Griep was a patient at McKee Medical Center, a Banner facility in Loveland, Colorado. As a condition of his admission, Banner demanded, collected, and received Mr. Griep's PII and PHI, which Banner maintained in its data systems.

53. During Mr. Griep's stay at McKee Medical Center, his debit card, which he holds jointly with his wife, was used to purchase food and beverages at the facility's

cafeteria. As part of that transaction, Banner collected and received Mr. Griep's PCI, which Banner maintains in its data systems.

54. On or about August 3, 2016, Mr. Griep received a letter from Banner informing him that his PII and PHI may have been compromised as a result of the data breach. Following his notification of the breach, Mr. Griep enrolled in the one-year credit monitoring service offered through Kroll.

55. Mr. Griep now lives in fear of further unauthorized misuse and exploitation of his confidential information, theft, and related financial fraud and resulting harm. Mr. Griep has spent and will spend time and money safeguarding his personal and private information from this cyber-attack, mindful that his information continues to remain at high risk for fraud, including continuing identity theft, and the continuing risk of being victimized by reason of Banner's conduct.

II. Defendant

56. Defendant Banner Health is an Arizona corporation with its principal place of business in Phoenix, Arizona.

JURISDICTION AND VENUE

57. This Court has jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d). The aggregated claims of individual Class Members exceed the sum or value of $5,000,000, exclusive of interests and costs, and members of the proposed classes are residents of different states.

58. This Court has jurisdiction over Banner because Defendant is incorporated in Arizona, is registered to conduct business in Arizona, has sufficient minimum contacts in Arizona, and otherwise intentionally avails itself of the markets in Arizona such that the exercise of jurisdiction by this Court is proper and necessary.

59. Venue is proper in this District under 28 U.S.C. § 1391(b) because a substantial part of the events or omissions giving rise to Plaintiff's claims occurred in this District.

FACTS

I. Banner Collects, Stores, and Accesses Sensitive Personal Information.

60. Banner is a Phoenix-based health system with annual revenue of approximately $7 billion. Banner and its subsidiaries own, control, and lease hospitals, clinics, nursing homes, clinical laboratories, ambulatory surgery centers, home health agencies, a captive insurance company, a foundation, an accountable healthcare organization, a Medicaid-managed health plan and related Medicare Advantage health plan, and other healthcare-related organizations. Banner also holds a 51 percent controlling interest in Sonora Quest Laboratories and a 50 percent non-controlling interest in Veritage LLC. Banner Health includes Banner Pharmacy Services, a network of clinical pharmacists, retail pharmacies, home delivery pharmacies, and specialty care pharmacies.

61. Banner offers comprehensive health services, physician services, hospice, and home care. As of December 21, 2016, Banner had over 200 Banner Centers and Clinics, 28 acute care hospitals including three academic centers, and 32 urgent care centers. During the relevant time period, Banner operated hospitals, clinics, and other related health entities in Alaska, Arizona, California, Colorado, Nebraska, Nevada, and Wyoming.

62. Banner oversees the provision of health network services under contract with various governmental and private commercial health insurers, including programs in conjunction with the following insurers: Blue Cross Blue Shield of Arizona, BCBS of Arizona Medicare Advantage and Alliance exchange plans, Medicare Advantage, Cigna, Aetna, and Health Net Medicare advantage. Banner acquired the University of Arizona Health network and its wholly owned subsidiary University Medical Center Corporation on February 28, 2015. This acquisition included a hospital in Tucson, a faculty practice plan, a Medicaid managed care health plan, and a related Medicare Advantage health plan. More than 400,000 members are currently served by the Banner provider networks.

63. Banner currently employs more than 50,000 employees and 7,000 physicians and medical staff members in six states, is Arizona's largest private employer, and is one of Northern Colorado's largest employers. A subset of Banner's employees enter into non-contributory retirement and death benefit plans. Employees also have health, dental, and long-term disability plans.

64. As part of its business, Banner collects, receives, stores, and accesses sensitive personal information from a variety of people, including customers, patients, insureds, and plan beneficiaries, as well as providers and employees.

65. The sensitive, confidential information that Banner collects includes PCI, which is data that Banner receives in connection with debit and credit card transactions; PII, which includes names, dates of birth, social security numbers, member identification numbers, home addresses, telephone numbers, and financial information; and PHI, which includes clinical and medical claims information.

66. Banner's employees, including providers and other healthcare professionals, provide PII to Banner in conjunction with beginning and continuing their employment. This information include names, addresses, telephone numbers, dates of birth, social security numbers, financial information, tax information, and professional credential information. For those who sign up for employment benefits, including health and life insurance, Banner employees also provide their beneficiaries' PII.

67. Banner also receives and obtains PII and PHI from its patients, including from minors. This information includes patients' names, addresses, telephone numbers, dates of birth, social security numbers, employer name and contact information, marital status, health and pharmaceutical histories, insurance information, and detailed treatment information. For some or all patients and insureds, Banner receives financial information relating to the patients' and insureds' salaries and assets.

68. Banner is also a health insurance provider, with approximately one billion dollars in annual insurance revenue. Banner insureds provide PII and PHI to Banner, including names, addresses, phone numbers, dates of birth, social security numbers,

financial information, health and pharmaceutical histories, and detailed treatment information. Banner also receives PII for plan beneficiaries.

69. Banner operates food and beverage outlets at many of its locations. People who make purchases at those outlets often do so using credit and debit cards. Using such payment methods, customers provide Banner with sensitive PCI, including information from driver's licenses and ID cards and what is known as "Track 1" and "Track 2" data. These tracks correspond to the horizontal location of the data within the magnetic strips on standard credit cards and include the credit card account number, credit card type, account holder name, expiration date, service code, and "discretionary" data such as the PIN and card verification value or verification code, which is the anti-fraud security feature used in "card not present" transactions and appears on most major credit and debit cards in the form of a three- or four-digit code.

II. Banner Was Obligated to Safeguard the PII, PHI, and PCI Entrusted to It.

A. Banner's Obligations under Federal and State Law to Safeguard PII, PHI, and PCI.

70. As a health plan and healthcare provider that transmits health information in electronic form, Banner is an entity covered by the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), *see* 54 C.F.R. § 160.102, and must comply with the HIPAA Privacy Rule and Security Rule, *see* 45 C.F.R. Part 160 and Part 164, Subparts A and E (setting forth "Standards for Privacy of Individually Identifiable Health Information").

71. HIPAA's Privacy Rule, otherwise known as "Standards for Privacy of Individually Identifiable Health Information," establishes national standards for the protection of health information.

72. HIPAA's Security Rule, otherwise known as "Security Standards for the Protection of Electronic Protected Health Information," establishes national security standards for the protection of health information that is held or transferred in electronic form.

73. HIPAA limits the permissible uses of "protected health information" and prohibits the unauthorized disclosure of "protected health information." 45 C.F.R. § 164.502. HIPAA requires that covered entities implement appropriate safeguards for this information. *See* 45 C.F.R. § 164.530(c)(1).

74. During the relevant time period, HIPAA obligated Banner to implement technical policies and procedures for electronic information systems that maintain electronic protected health information so that such systems were accessible only to those persons or software programs that had been granted access rights. *See* 45 C.F.R. § 164.312(a)(1).

75. During the relevant time period, HIPAA obligated Banner to protect against any reasonably anticipated threats or hazards to the security or integrity of electronic protected health information. *See* 45 CFR § 164.306(a)(2).

76. During the relevant time period, HIPAA also obligated Banner to implement policies and procedures to prevent, detect, contain, and correct security violations, *see* 45 C.F.R. § 164.306(a)(1), 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)(3).

77. During the relevant time period, HIPAA obligated Banner to ensure that its workforce complied with HIPAA security standard rules, *see* 45 C.F.R. § 164.306(a)(4), to effectively train its workforce on the policies and procedures with respect to protected health information, as necessary and appropriate for those individuals to carry out their functions and maintain the security of protected health information, 45 C.F.R. § 164.530(b)(1).

78. The Office for Civil Rights ("OCR"), within the Department of Health and Human Services ("HHS"), issues guidance to assist HIPAA-covered entities.[2] For example, the guidance regarding Risk Analysis clarifies the expectations of organizations

[2] *See* US Department of Health & Human Services, Security Rule Guidance, http://www.hhs.gov/hipaa/for-professionals/security/guidance/index.html (last visited February 19, 2017).

required to meet the Security Rule requirements, including by providing information on risk analysis requirements, elements of risk analysis, and a list of resources for covered entities to access.[3] 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."

79. Banner is prohibited by the Federal Trade Commission Act, 15 U.S.C. § 45, from engaging in "unfair or deceptive acts or practices in or affecting commerce." The FTC has determined that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" under the Act.

80. Banner is also an entity covered by The Gramm-Leach-Bliley Act, 15 U.S.C. § 6801, *et. seq*. Thus, Banner had an "affirmative and continuing obligation to respect the privacy of its customers and to protect the security and confidentiality of those customers' nonpublic personal information." 15 U.S.C. § 6801.

81. As described below, Banner is also obligated by various state laws and regulations to protect Plaintiffs' and Class Members' sensitive, confidential information.

82. Various state statutes obligate Banner to treat the information of Plaintiffs and the Class Members confidentially and to protect it from disclosure, including but not limited to:

a. Alaska Stat. §§ 21.07.040 and 18.23.100 required Banner to treat medical and financial information as confidential and required it to protect medical records from unauthorized access;

b. A.R.S. §§ 36-509 and 36-2221(D) required Banner to keep medical records and information confidential;

[3] *See* US Department of Health and Human Services, Final Guidance on Risk Analysis, http://www.hhs.gov/hipaa/for-professionals/security/guidance/final-guidance-risk-analysis/index.html (last visited February 19, 2017).

c. Cal. Civ. Code § 1798.81.5(b) and Cal. Health & Safety Code § 1280.18 (a) required Banner to implement and maintain reasonable security procedures and to protect and safeguard PII and PHI from unauthorized access;

d. Neb. Rev. Stat. §§ 44-4110.01, 44-4725, 44-7210, 44-4725, 44-32, 172, 38-1225, and 44-901 et seq. required Banner to maintain the confidentiality of PII and PHI; and

e. Nev. Rev. Stat. § 439.590 required Banner to maintain the confidentiality of PHI.

83. In addition to the foregoing obligations imposed by federal and state law, Banner owes a common law duty to individuals who entrusted Banner with sensitive PII, PHI, and PCI to exercise reasonable care in receiving, maintaining, storing, and deleting that information in Banner's possession. Banner owed a duty to prevent PII, PHI, and PCI from being compromised, lost, stolen, accessed, or misused by unauthorized third parties. Part and parcel of Banner's duty were the obligations to provide reasonable security consistent with industry best practices and requirements and to ensure information technology systems and networks, and the personnel responsible for those systems and networks, adequately protected the PII, PHI, and PCI Plaintiffs and the Class Members entrusted to it.

84. Banner owes a duty to Plaintiffs and the Class Members, who entrusted Banner with their sensitive PII, PHI, and PCI to design, maintain, and test the information technology systems that housed that information and to ensure that the information was adequately secured and protected.

85. Banner owes a duty to Plaintiffs and the Class Members to create, implement, and maintain reasonable data security practices and procedures sufficient to protect the PII, PHI, and PCI stored and accessed in Banner's data systems. Among other things, this duty requires Banner to adequately train employees and others with access to the information on the procedures and practices necessary to safeguard it.

86. Banner owes a duty to Plaintiffs and the Class Members to implement processes that would enable Banner to timely detect a breach of its information technology systems.

87. Banner owes a duty to Plaintiffs and Class Members to act upon data security warnings and red flags in a timely fashion.

88. Banner owes a duty to Plaintiffs and the Class Members to disclose when and if its information technology systems and data security practices were not adequate to protect and safeguard PII, PHI, or PCI.

89. Banner owes a duty to Plaintiffs and the Class Members to timely disclose the fact that a data breach had occurred.

90. Banner owes these duties to Plaintiffs and the Class Members because they are foreseeable and probable victims of Banner's inadequate data security practices. Banner collected and received their PII, PHI, and PCI and knew that a breach of its data systems would cause proposed Class Members to incur damages and, as detailed below, knew or should have known that its data systems were a prime target for cyberattack.

B. Banner's Promises to Safeguard PII, PHI, and PCI.

91. In collecting PII, PHI, and PCI from its patients, insurance plan members, plan beneficiaries, customers, providers, and/or employees, Banner explicitly and implicitly promised, represented, and warranted that it would protect the privacy and confidentiality of that information.

92. Banner understands that patients, insurance plan members, plan beneficiaries, and other Banner customers, as well as Banner's providers and employees, place a premium on privacy, especially as it pertains to sensitive health-related, personal, and financial information.

93. Banner provides its patients and insureds with a notice of privacy practices and other privacy statements. As discussed below, Banner also dedicates a section of its website to explaining its privacy and data collection policies. This is consistent with the National Association of Insurance Commissioners Roadmap for Cybersecurity Consumer

Protections, which tells consumers to "[e]xpect insurance companies/agencies to have a privacy policy posted on their websites and available in hard copy, if you ask. The privacy policy should explain what personal information they collect, what choices consumers have about their data, how consumers can see and change/correct their data if needed, how the data is stored/protected, and what consumers can do if the company/agency does not follow its privacy policy."

94. At all relevant times, Banner maintained and promulgated privacy policies through which Banner committed to maintaining and protecting the confidentiality of information that Banner and its affiliates collected in the course of doing business.

95. Banner's website contains a "Privacy Practices for Banner Health" page that states: "Banner is committed to protecting the confidentiality of information about you, and is required by law to do so. This notice describes how we may use information about you within Banner and how we may disclose it to others outside Banner. This notice also describes the rights you have concerning your own health information. Please review it carefully and let us know if you have questions."

96. The language quoted in the preceding paragraph, including that "Banner is committed to protecting the confidentiality of information about you, and is required by law to do so," is repeated within Banner's Notice of Privacy Practices, which is linked on the same webpage.

97. Banner has posted the Notice of Privacy Practices online since at least September 2013. Banner provides the Notice of Privacy Practices to all patients and insurance plan members when they first enter contractual relationships with Banner, and the notice is incorporated by reference in Banner's patient registration forms. It thus forms part of the contract between Banner and the patients who receive treatment or other services at Banner hospitals, clinics, and other facilities, as well as Banner's insurance plan members.

98. The Notice of Privacy Practices states that it "applies to Banner facilities and its personnel, volunteers, students, and trainees" as well as "to other health care

providers that come to the facility to care for patients, such as physicians, physician assistants, therapists, emergency services providers, medical transportation companies, medical equipment suppliers, and other health care providers not employed by Banner unless these health care providers give you their own Notice of Privacy Practices." It also states that "Banner is required by law to give you this Notice and to follow terms of the Notice that is currently in effect."

99. The Notice of Privacy Practices lists a limited set of situations in which personal information can be disclosed, including for research, operational, public safety, and other express reasons. According to the policy, "[o]ther uses and disclosures not described in this Notice will be made only with your written authorization…." On information and belief, Banner maintained and promulgated prior versions of this confidentiality notice beginning at least as early as 1996, after HIPAA was enacted, and each such version of the notice contained a similar commitment to protect the PII and PHI of patients, healthcare plan members, and beneficiaries.

100. Banner Health's Medical Treatment Agreement contains a "Release of Information" clause, stating: "The patient acknowledges and agrees that medical and/or financial records . . . may be provided to" healthcare providers, researchers for medical purposes, individuals, and entities "as specified by federal and state law and/or in Banner's Notice of Privacy Practices," and within Banner for appropriate patient care. All patients are required to affirm: "I have received the Notice of Privacy Practices."

101. Banner's Condition of Admission and Treatment form also contains an acknowledgment that the patient or representative was required to initial: "I acknowledge receipt of or I have personally received and decline another copy of the: Notice of Privacy Practices for Banner."

102. In its Behavioral Health Clients Rights document, Banner promises that the patient has the right "[t]o have the client's information and records kept confidential and released only as permitted under R9-20-211(A)(3) and (B)." The same document provides that the patient has the right "[t]o privacy in treatment …."

103. Banner provides a document titled "Privacy Practices in Banner Plans" to its insureds. The document contains substantially similar language in relevant part as the Notice of Privacy Practices referenced above, and it forms part of the contract between Banner and all of Banner's insurance health plan members. The document states it is a "notice [that] describes how medical information about you may be used and disclosed and how you can get access to this information." The document states that

> Banner is committed to protecting the confidentiality of information about you, and is required by law to do so. This Notice describes how we may use information about you within Banner as Plan Administrator of the Banner and Dental Plans (the "Plan") and how we may disclose it to others outside Banner. We will notify you if there is a breach of your unsecured protected health information.

It goes on to state the limited circumstances in which Banner will disclose personal information; for example, it states:

> **Payment:** Banner may use and disclose your information to obtain payment for the medical services rendered to you and the supplies you have received. For example, the Plan may request to see parts of your medical record before it will pay Banner or other providers for your treatment and related supplies. The Plan may need information regarding treatment and services you are going to receive to meet prior approval/pre-certification requirements or to determine whether the treatment will be covered under the Plan.

It also states that "Other uses and disclosures not described in this Notice will be made only with your written authorization. You may revoke such authorization by sending us a written request." Finally, it states that "Banner is required by law to give you this Notice and to follow terms of the Notice that is currently in effect."

104. Banner also provides a Summary Plan Description booklet to its insureds. The booklet contains, among other things, a section entitled "Privacy of Personal Health Information." That section states:

> Banner, as Plan sponsor, is committed to protecting your private and personal health information. Banner has and will continue to enter into agreements with service providers, referred to as 'business associates,' that contractually protect your personal health information under the same guidelines as those used by Banner. Banner will not disclose your personal health information without your prior written consent or authorization, except as necessary for your treatment, payment for services recorded, health care operations or as otherwise permitted by law. Additionally, you have the right to access and review your own personal health information in

> accordance with procedures established by Banner and presented in the Notice of Privacy Practices issued separately.

The booklet also states that it

> is incorporated into and part of the Master Health and Welfare Plan. Complete details of the Master Health and Welfare Plan, however, are not set forth in this booklet and the legal documents which constitute this document will govern. If there is any difference between this booklet and those of the Master Health and Welfare Plan Document the Plan Administrator will apply the Master Health and Welfare Benefit Plan Document and this booklet in a consistent manner.

The booklet forms part of the contract between Banner and all of Banner's insurance health plan members.

105. In its internal policies, Banner has acknowledged "confidentiality is vital to effective credentialing, peer review and quality assessment/improvement activities," and that "any breach of the confidentiality of … credentialing" constitutes a failure to meet certain professional and ethical standards.

106. Banner publishes an Employee Handbook, which it provides to its employees.

107. The Employee Handbook states:

> Banner is in the business of caring for and providing services to patients and their families. Patient care information is considered confidential by law and we have an obligation to protect our patients' rights to confidentiality. … Any materials developed by employees during work hours will remain the property of Banner and are to be considered confidential information. … Our obligation to protect confidential information is so important that every employee is expected to honor privacy and confidentiality.

108. The Employee Handbook also states:

> The Health Insurance Portability and Accountability Act (HIPAA) is a federal law that applies to health plans, health care providers, and health care clearinghouses. Banner adheres to HIPAA as it applies to our activities as a health care provider and health plan, and employees are expected to comply with HIPAA as well. The HIPAA legislation focuses on the following three major areas: Privacy – provides rules in regard to how an individual's health information may be used and disclosed. Transactions and Code Sets – requires the use of standard transaction formats and code sets when an individual's financial health information is transmitted electronically. Security – requires specific security measures to be in place to protect an individual's health information that is sent or stored electronically. Banner provides employee education on HIPAA during employee orientation and annually through mandatory education. Violations of HIPAA are very serious and may result in corrective action, up to and including termination.

109. The Employee Handbook is based on and expressly references internal policies and procedures that govern the conduct of both Banner and its employees. One such policy is the Banner Workforce Confidentiality Policy. That policy states its purpose is to "protect confidential information," and it states "Banner has a legal and ethical responsibility to safeguard confidential information. Banner will comply with all laws and regulations relating to confidentiality and will protect oral, paper, and electronic confidential information." The same policy states that it "[a]pplies to all Banner workforce including employees, professional and medical staff, volunteers and students," and repeats some of the Employee Handbook language quoted above, including "Banner's obligation to protect confidential information is so important that every member of Banner must agree to honor privacy and confidentiality during and beyond employment."

110. The Employee Handbook and incorporated policies form part of the contract between Banner and all of Banner's employees.

111. Banner, either directly or through a wholly-owned subsidiary, enters into employment agreements with its physicians. On information and belief, the terms of those agreements are, in relevant part, the same or materially the same. The agreements prohibit the physician employees from disclosing patient information and other sensitive, non-public information. The agreements state that it is the intent of the parties to the agreement to comply in all respects with all applicable federal, state, and local laws, regulations, rules, and interpretive case decisions, and that the parties structured their relationship with that specific intent. The agreements require the physician employees to authorize the release to Banner or its wholly-owned subsidiary all reports, records, and other information pertaining to the physician employee; in exchange, Banner and/or its wholly owned subsidiary agree to treat such information in a confidential manner.

112. The aforementioned express contracts included implied terms requiring Banner to implement data security adequate to safeguard and protect the confidentiality of Plaintiffs' and Class Members' PII and PHI, including but not limited to in accordance with HIPAA regulations, federal, state, and local laws, and industry standards.

113. Data security – as set forth in Banner's Notice of Privacy Practices, its Medical Treatment Agreement, its Condition of Admission and Treatment form, its Behavioral Health Clients Rights document, its Privacy Practices in Banner Plans document, its Summary Plan Description booklet, its Employee Handbook, and various other of Banner's internal policies – was an essential implied term of the express contracts alleged above and herein.

114. Such implied terms required that Banner protect Plaintiffs' and Class Members' PII and PHI and prevent unauthorized access to such information.

115. No reasonable person would have provided his or her PII, PHI, or PCI to Banner without an understanding that Banner would take reasonable steps to protect that information consistent with its promises, its legal obligations, and the implied terms of its express contracts.

C. Banner's Obligations under Industry Guidelines and Standards.

116. In early 2015, the National Association of Insurance Commissioners ("NAIC"), a standards-setting organization comprised of insurance regulators from across all U.S. jurisdictions, adopted twelve Principles for Effective Cybersecurity Insurance Regulatory Guidance. The NAIC principles highlight the importance of protecting sensitive personal data in the insurance sector. These principles broadly lay out practices, guidelines, and measures that the insurance industry should take to protect personal information. They include:

a. Principle 2: "Confidential and/or personally identifiable consumer information data that is collected, stored and transferred inside or outside of an insurer's, insurance producer's or other regulated entity's network should be appropriately safeguarded."

b. Principle 8: "Insurers … should take appropriate steps to ensure that third parties and service providers have controls in place to protect personally identifiable information."

c. Principle 9: "Cybersecurity risks should be incorporated and addressed as part of an insurer's … enterprise risk management (ERM) process. Cybersecurity transcends the information technology department and must include all facets of an organization."

d. Principle 10: "Information technology internal audit findings that present a material risk to an insurer should be reviewed with the insurer's board of directors or appropriate committee thereof."

e. Principle 11: "It is essential for insurers … to use an information-sharing and analysis organization (ISAO) to share information and stay informed regarding emerging threats or vulnerabilities, as well as physical threat intelligence analysis and sharing."

f. Principle 12: "Periodic and timely training, paired with an assessment, for employees of insurers… regarding cybersecurity issues is essential."

117. The PCI Security Standards Council is a global organization that maintains and promotes payment card industry standards for the safety of cardholder data. The council helps merchants understand and implement standards for security policies, technologies, and ongoing processes that protect their payment systems from breaches and theft of cardholder data. The council also helps vendors understand and implement standards for creating secure payment solutions. The Council promulgates standards, requirements, and guidance to merchants who accept payment cards in business transactions. Banner is a merchant subject to the Council's standards, requirements, and guidance.

118. The Council has warned merchants that the account number, cardholder name, expiration date, card verification value, and other data on Tracks 1 and 2 are "sensitive cardholder data"; that the data on Tracks 1 and 2 "must never be stored"; and that merchants must have "a good business reason" for storing any of the other sensitive cardholder data, in which case "that data must be protected." The Council further instructs merchants to "secure cardholder data where it is captured at the point of sale and

as it flows into the payment system. The best step you can take is to not store any cardholder data. This includes protecting … [p]oint of sale systems, … networks …, [and p]ayment card data storage and transmission."

119. Years ago, the Council issued the PCI Data Security Standard ("PCI DSS"), which applies to Banner and any other entity that stores, processes, or transmits cardholder data; any business that accepts or processes payment cards must comply with the PCI DSS.

120. According to the Council, "[m]ost aspects of the PCI DSS are already a common best practice for security." Research conducted by Verizon from 2011 through 2013 found that organizations that suffered a data breach were less likely to have been compliant with PCI DSS than other organizations.

121. To achieve compliance with the PCI DSS, an organization must meet all applicable PCI DSS requirements. The PCI DSS security requirements apply to all system components included in or connected to the cardholder data environment (including the people, processes, and technologies that store, process, or transmit cardholder data or sensitive authentication data).

122. The PCI DSS includes twelve requirements that specify the framework for a secure payments environment as follows:

PCI Data Security Standard – High Level Overview

Build and Maintain a Secure Network and Systems	1. Install and maintain a firewall configuration to protect cardholder data 2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	3. Protect stored cardholder data 4. Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	5. Protect all systems against malware and regularly update anti-virus software or programs 6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	7. Restrict access to cardholder data by business need to know 8. Identify and authenticate access to system components 9. Restrict physical access to cardholder data
Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data 11. Regularly test security systems and processes
Maintain an Information Security Policy	12. Maintain a policy that addresses information security for all personnel

123. With respect to "Requirement 1," the PCI DSS states:

> Firewalls are devices that control computer traffic allowed between an entity's networks (internal) and untrusted networks (external), as well as traffic into and out of more sensitive areas within an entity's internal trusted networks. The cardholder data environment is an example of a more sensitive area within an entity's trusted network. A firewall examines all network traffic and blocks those transmissions that do not meet the specified security criteria. All systems must be protected from unauthorized access from untrusted networks, whether entering the system via the Internet as e-commerce, employee Internet access through desktop browsers, employee e-mail access, dedicated connections such as business-to-business connections, via wireless networks, or via other sources. Often, seemingly insignificant paths to and from untrusted networks can provide unprotected pathways into key systems. Firewalls are a key protection mechanism for any computer network.

It states, further, that merchants must "[i]nspect the firewall and router configuration standards … and verify that standards are complete and implemented." Merchants must conduct firewall-rule-set reviews every six months.

124. With respect to Requirement 7, the PCI DSS states that restricting access to cardholder data by business need-to-know is required to "ensure critical data can only be accessed by authorized personnel, systems and processes" and systems "must be in place to limit access based on need to know and according to job responsibilities." It also requires that merchants "[e]stablish an access control system(s) for systems components that restricts access based on a user's need to know, and is set to 'deny all' unless specifically allowed," because "[w]ithout a mechanism to restrict access based on user's need to know, a user may unknowingly be granted access to cardholder data. Additionally, a default 'deny-all' setting ensures no one is granted access until and unless a rule is established specifically granting such access."

125. With respect to Requirement 10, the PCI DSS explains that "[l]ogging mechanisms and the ability to track user activities are critical in preventing, detecting, or minimizing the impact of a data compromise. The presence of logs in all environments allows thorough tracking, alerting, and analysis when something does go wrong." It further states, "[i]t is critical to have a process or system that links user access to system components accessed. This system generates audit logs and provides the ability to trace back suspicious activity to a specific user." It also requires that merchants maintain

access to all audit trails because "[m]alicious users often attempt to alter audit logs to hide their actions, and a record of access allows an organization to trace any inconsistencies or potential tampering of the logs to an individual account."

126. According to the Council, the essence of the overall Standard

> is three steps: Assess, Remediate and Report. **Assess** is the process of taking an inventory of your IT assets and business processes for payment card processing, and analyzing them for vulnerabilities that could expose cardholder data. **Remediate** is the process of fixing those vulnerabilities. **Report** entails the compilation of records required by PCI DSS to validate remediation, and submission of compliance reports to the acquiring bank and card payment brands you do business with. Doing these three steps is an ongoing process for *continuous* compliance with the PCI DSS requirements.

(All emphasis in original.)

127. With respect to the "Assess" step, the Council instructs: "The primary goal of assessment is to identify all technology and process vulnerabilities posing a risk to the security of cardholder data that is transmitted, processed or stored by your business. … Determine how cardholder data flows from beginning to end of the transaction process…." The Council tells merchants that "risk assessments can identify areas containing data that need protection versus areas that are more open and do not need access to sensitive data."

128. The PCI DSS requires merchants to perform risk assessments. Risk assessments are formal processes organizations use to identify threats and vulnerabilities that could negatively impact the security of cardholder data. According to the Council, during "a risk assessment, all vulnerabilities should be considered. … Vulnerabilities may be identified from vulnerability assessment reports, penetration-test reports and technical security audits such as firewall rule reviews, secure code reviews and database configuration reviews." The Council provides a table of "examples of threats and vulnerabilities," which it emphasizes "is not an exhaustive list." The table lists the first example threat as "hackers, malicious individuals, cyber criminals," identifies the first potential vulnerability as "Lack of network security—e.g., properly configured firewalls, lack of intrusion detection," and warns that, if that vulnerability is exposed, it could lead

to "Network intrusion," "System compromise," "Compromise of sensitive data," and "Theft of CHD [cardholder data]."

129. The PCI DSS states that the "first step" of an assessment is to accurately determine the scope of the review. This requires "identifying all locations and flows of cardholder data, and identify[ing] all systems that are connected to or, if compromised, could impact the CDE [cardholder data environment] (for example, authentication servers) to ensure they are included in the PCI DSS scope. All types of systems and locations should be considered as part of the scoping process, including backup/recovery sites and failover systems."

130. With respect to the "Remediate" step, the Council instructs: "Remediation is the process of fixing vulnerabilities—including technical flaws in software code or unsafe practices in how an organization processes or stores cardholder data. Steps include: … Review and remediation of vulnerabilities found in on-site assessment (if applicable) or through the self-assessment process. … [and] Applying patches, fixes, workarounds, and changes to unsafe processes and workflow."

131. The Council instructs merchants to "understand where payment card data flows for the entire transaction process" and to "not store cardholder data unless it's absolutely necessary." The Council further instructs merchants to "use strong cryptography to render unreadable cardholder data that [they] store, and use other layered security technologies to minimize the risk of exploits by criminals," and to "not locate servers or other payment card system storage devices outside of a locked, fully-secured and access-controlled room."

132. The PCI DSS "strongly recommend[s]" "isolating (segmenting)[ ] the cardholder data environment from the remainder of an entity's network." The PCI DSS states that doing so may reduce the "risk to an organization."

133. According to the Council, best practices in PCI security include: "Prior to any modification to the [cardholder data] environment, all the systems and networks affected by the change—including any new systems—should be identified. Questions that

should be considered include: 'Do the changes introduce new connections between systems in the CDE [cardholder data environment] and other systems that could bring additional systems or networks into scope for PCI DSS?' Other special considerations should also be given to how the proposed change may affect technologies or any underlying infrastructure that supports the security of the CDE, such as changes to network-traffic routing rules, firewall rules, DNS configurations, or other security-related functions."

D. Banner's Patients, Insureds, and Other Customers, as Well as Its Healthcare Providers and Employees, Reasonably Expected That Banner Would Safeguard Their PII, PHI, and PCI.

134. Banner promised to Plaintiffs and the Class Members that it was committed to protecting the confidentiality of their sensitive information they entrusted to it and that it is required by law to do so.

135. Healthcare patients and insurance plan members and beneficiaries are generally aware of HIPAA as well as the fact that it and other laws and standards require hospitals, clinics, and other health facilities to safeguard their PHI from unauthorized disclosure.

136. The PCI Security Standards Council has stated that "[t]he public expects that merchants … will protect payment card data to thwart data theft and prevent unauthorized use."

137. Patients who visited Banner facilities, along with Banner healthcare providers, employees, insurance plan members and beneficiaries, and customers, reasonably expected that Banner was taking appropriate steps to safeguard the sensitive, confidential information with which it is entrusted, including PII, PHI, and PCI.

138. Indeed, Plaintiffs and the Class Members would not have provided their PII, PHI, and PCI to Banner without an express understanding and belief that Banner would take appropriate steps to safeguard and protect their sensitive, confidential information, including PII, PHI, and PCI.

139. At no time during the relevant time period did Banner disclose that its information security was inadequate to reasonably safeguard the PII, PHI, and PCI to which Banner was entrusted. Nor did Banner disclose that it had failed to follow the [redacted] with respect to the protection of sensitive information, [redacted]. As Banner knew, such a disclosure would have been material and contrary to the existing understanding of the patients, insureds, and other customers of Banner, as well as Banner's healthcare providers and employees.

III. Banner Knew Its Data Systems Were at High Risk of Cyber Attack.

140. Throughout the relevant time period, Banner has had electronic data systems that maintain, transmit, and otherwise utilize the PII, PHI, and PCI to which Banner is and has been entrusted by its patients, insurance plan members, other customers, providers, and employees.

141. Banner has long known these data systems are high value targets for cyber criminals and at high risk for a data breach.

142. The information security risks for health and insurance providers like Banner stem in large part from the value of the data they hold. Healthcare data is highly valuable on the black market, where it is traded, sold, and re-sold through websites, secret chat rooms, and underground forums. Those who acquire the information can profit from it at the expense of the breach victims. Information regarding things like date of birth and social security number are particularly tied to the identity of an individual and are not easily changed; thus, they are highly useful to perpetrate identify theft and other types of frauds. Medical information is even more highly valuable and is reportedly "worth 10 times more than [a person's] credit card number on the black market." Some estimates put medical-identity information, including health insurance credentials, as having values of up to $1,000 per record. Because of its value, this type of information is an attractive target for hackers and cybercriminals.

143. Because they collect and possess large amounts of this valuable information, healthcare service providers and insurance companies face unique—though highly publicized and well-understood—risks relating to cybersecurity.

144. As a result, cybersecurity has been a topic of increased focus by the healthcare and insurance industries for years.

145. Both the threats posed by and awareness of the risk of data breaches in the healthcare and insurance industries have skyrocketed, with massive breaches affecting healthcare organizations and health insurers like Anthem, Inc. (in 2014-2015), Premera Blue Cross (in 2014-2015), Excellus Health Plan, Inc. (in 2013-2015), Community Health Systems, Inc. (in 2014), UCLA Health, and 21st Century Oncology. The likelihood of criminal cyberattacks for healthcare organizations doubled from 2009 to 2013, per one survey.

146. Daniel Nutkis, the chief executive of the Health Information Trust Alliance, a healthcare industry group that works with companies to improve data security, said in 2015 that "the industry has become, over the last three years, a much bigger target."

147. A 2015 Raytheon study found that healthcare organizations are 340 percent more likely to be impacted by an information security incident than other sectors, and twice as likely to experience data theft from cyber criminals. Data breaches have cost the healthcare industry $6.2 billion annually in recent years.

148. In December 2012, the Ponemon Institute issued its Third Annual Benchmark Study on Patient Privacy and Data Security. The study, which included data from 80 participating healthcare organizations, found that cyberattacks were involved in approximately 33 percent of all healthcare data breaches. The healthcare companies themselves generally "agree[d] that patients are at a greater risk of financial identity theft if their records are lost or stolen." The Institute's 2013 report reached similar conclusions.

149. On April 8, 2014, the Federal Bureau of Investigation ("FBI") Cyber Division issued a Private Industry Notification to healthcare providers, warning them that their cybersecurity systems are inadequate. Per the notification, "the health care industry

is not technically prepared to combat against cyber criminals' basic cyber intrusion tactics, techniques and procedures (TTPs), much less against more advanced persistent threats (APTs)" and "is not as resilient to cyber intrusions compared to the financial and retail sectors, therefore the possibility of increased cyber intrusions is likely." The notification warned that cyberattacks against healthcare systems would increase due in part to "mandatory transition from paper to electronic health records" and "a higher financial payout for medical records in the black market." The FBI also noted that it "has observed malicious actors targeting healthcare related systems, perhaps for the purpose of obtaining Protected Health Information (PHI) and/or Personally Identifiable Information (PII)."

150. The FBI notification cited a report prepared by the SANS Institute warning the healthcare industry that it was not adequately prepared to combat data breaches. The report analyzed data collected between September 2012 and October 2013 and found the results "alarming." The report explained the data "not only confirmed how vulnerable the industry had become, it also revealed how far behind industry-related cybersecurity strategies and controls have fallen."

151. In August 2014, after one of the largest hospital organizations in the nation, Community Health Systems, Inc., experienced a data breach, the FBI warned the healthcare industry that hackers were targeting them: "The FBI has observed malicious actors targeting healthcare related systems, perhaps for the purpose of obtaining Protected Healthcare Information (PHI) and/or Personally Identifiable Information (PII)."

152. In the fall 2014 national meeting of the NAIC, a Prudential Insurance Vice President gave a presentation entitled "Cybersecurity & Insurance Companies." The presentation warned of the imminent threat to insurance companies' data systems from third-party threats. The presentation quoted U.S. Attorney General Eric Holder: "From criminal syndicates, to terrorist organizations, to foreign intelligence groups, to disgruntled employees and other malicious intruders, the range of entities that stand ready

to execute and exploit cyberattacks has never been greater." The same presentation contained a warning from the FBI director about the imminent risk of cyberattacks.

153. In response to the NAIC's issuance of the insurance industry cybersecurity principles discussed above in 2015, PricewaterhouseCoopers published an article entitled, "Cybersecurity regulatory guidance for the insurance sector." The article highlighted that it was "important to note that the NAIC's action was unsurprising. High-profile data breaches at several health insurance providers exposed data on 90 million consumers, revealing the industry's vulnerability. … It's time for insurance companies to play catch-up, and NAIC is spurring them on."

154. Robert Rost, Banner's IT Operations Director of Defensive Services, gave a conference presentation in March 2016 with others. The presentation explained that electronic health record theft is a "[r]eal and growing threat to healthcare in 2016." It noted that "[e]xternal attacks are getting more sophisticated," and may be perpetrated through "[o]rganized crime."

IV. Banner Knew Its Information Security Was Inadequate.

155. Since at least 2012, Banner's information security measures have been objectively unreasonable and deficient—particularly in light of healthcare, insurance, and payment card industry standards, applicable legal requirements, and the known and growing threat to healthcare and insurance companies from cybercriminals.

156. Best practices have long required the use of multi-factor authentication for remote access to computer networks that contain sensitive information. Instead of using just one form of authentication, such as a password, multi-factor authentication requires the user to authenticate using at least two separate identifiers, such as a password and a separate, system-generated passcode sent to a known user location or device (such as the user's cellular phone). This provides a significantly more secure environment because even if a password becomes compromised, the password alone will not suffice to gain access to the network.

157. Because hackers frequently compromise systems and databases that use simple, single-factor authentication, the top security publications in the years leading up to June 2016 consistently recommended that high-value targets be secured with multi-factor authentication. The Center for Internet Security, Australian Signals Directorate, Verizon Enterprise Solutions Data Breach Investigations Report, and NSA's Information Assurance Directorate all recommend two-factor authentication be implemented to secure privileged accounts and remote access. In fact, the 2013 Verizon Data Breach Investigations Report concluded that up to 80 percent of past hacks could have been prevented if multi-factor authentication had been in place.

158. Hackers often target remote access solutions (used to access the network) as well as privileged accounts (needed for broader network access).

159. [redacted]

160. Another recommended form of network protection is application whitelisting, which limits the applications that can be used on a server to only those appearing on a preapproved list. Whitelisting essentially prevents malware applications from being run on the system device, inhibiting and potentially stopping hackers from being able to use their hacking tools. The NIST guidelines call for application whitelisting in high-risk environments. It is the most important information security control per the NSA's Information Assurance Directorate and the Australian Signals Directorate and the second most important per the SANS Institute. Application whitelisting is among the four controls that the Australian Signals Directorate says would

prevent 85 percent of cyber-intrusions. [redacted]

161. Best practices have long called for networks like Banner's to employ ingress and egress monitoring, logging, and filtering. Ingress filtering prevents receipt of unwanted traffic (including attack packets) into a network. Egress filtering reviews data leaving the network and prevents the transmission outside the network of any information not unauthorized to leave. Ingress and egress monitoring and logging detect and record the entry into and movement across systems. [redacted]

162. [redacted]

163. Security experts have increasingly emphasized the need to reduce "dwell time," the period in which hackers can explore networks before being detected and eliminated. Time is a critical factor in data breaches—the longer hackers are able to access and move inside networks, the greater their opportunity to locate and obtain sensitive information. Thus, delays in detection and response increase the likely severity of a breach. Network monitoring, logging, and alert systems can detect unusual activity or failures and alert IT security personnel to take appropriate action. Logging is thus an essential component of any network security regiment because network logs provide incident response personnel the ability to identify, analyze, diagnose, respond to, and mitigate any anomalous network traffic.

164. Up to and including June and July 2016, Banner's network failed to comply with all 12 PCI DSS requirements. [redacted]

165. [redacted] Such monitoring is standard in the industry, and operating without it was unreasonable. The monitoring helps identify potentially suspicious actions and access by unauthorized users within Banner's network; early detection of such activity can stop and minimize the likelihood of improper data exfiltration.

166. Deloitte & Touche LLP ("Deloitte"), which is a leader in providing security-specific advisory services to help companies assess, analyze, and improve their information security. Deloitte is paid for its cybersecurity assessments by the companies it assesses. On information and belief, Deloitte prepares the assessments and written recommendations in a way designed to document its clients' information security deficiencies while seeking to avoid creating a record that could be used against the companies in subsequent litigation in the event of a cyberattack.

167. [redacted]

168. [redacted]

169. [redacted]

[redacted]

170. [redacted]

[redacted]

171. [redacted]

[redacted] Banner failed to thoroughly investigate and harden their systems against the identified risks up to and through the 2016 data breach.

172. [redacted]

[redacted]

173. [redacted]

[redacted]

[redacted]

174. [redacted]

[redacted]

175. [redacted]

[redacted] Banner failed, however, to undertake those remedial measures up to and through the 2016 data breach.

176. [redacted]

[redacted]

[redacted]

177. [redacted]

[redacted]

178. [redacted]

[redacted]

179. [redacted]

[redacted]

180. [redacted]

[redacted]

a. [redacted]

[redacted]

i. [redacted]

- [redacted]
- [redacted]
- [redacted]

[redacted]

ii. [redacted]

[redacted]

b. [redacted]

i. [redacted]

[redacted]

ii. [redacted]

[redacted]

c. [redacted]

[redacted]

i. [redacted]

[redacted]

[redacted]

ii. [redacted]

[redacted]

d. [redacted]

[redacted]

e. [redacted]

i. [redacted]

[redacted]

[redacted]

f. [redacted]

181. [redacted]

182. To address the issues identified in its 2014 assessment, [redacted]

183. [redacted]

[redacted] For example, in 2016, Banner [redacted] failed to segment the network and information on its network. [redacted] Banner also did not establish an office of the Chief Information Security Officer until after the data 2016 breach, with system level responsibility for information security at Banner.

184. [redacted]

185. [redacted] thus, rather than exhibiting improvement in its information security, Banner was moving in the wrong direction.

186. [redacted]

187. [redacted]

188. [redacted] Utilization of these "off the shelf" patches are a fundamental aspect of network security; such patches often include security updates that help protect the affected systems from unauthorized access and close known and publicized security vulnerabilities. [redacted]

189. [redacted]

[redacted]

190. [redacted]

191. Prior to July 2016, Banner failed to remediate its security issues despite several prior exposed failures on its part to protect PII and PHI. In 2014, Banner exposed the Medicare identification and social security numbers of more than 50,000 people to public view. Per a spokesperson, the error was caused by a problem with how Banner processed mailing lists for its quarterly magazine. Using sensitive information like social security numbers to organize mailing lists reflected a culture of reckless disregard of data security. Also in 2014, the MyBanner portal experienced a data breach, in which patient data was exposed to incorrect users. In response to the breach, senior management, IT security, and the compliance group were not notified until about a month after the breach was discovered.

192. Banner's failures to protect PII, PHI, and PCI during the relevant time period were such that no reasonable person would have provided such information to Banner had they known of the significant flaws in Banner's information-security systems, as disclosed in the various reports.

V. Hackers Exploit Banner's Inadequate Information Security in Data Breach.

193. A targeted threat actor, [redacted] gained access to Banner's network in June and July 2016. The hackers accessed Banner's systems and copied and removed PII, PHI, and PCI; they were able to do so only because Banner failed to employ the reasonable information security precautions recommended by [redacted] and otherwise discussed in this Complaint.

194. [redacted]

195. [redacted]

196. [redacted]

197. The hackers first gained access to Banner's network on June 17, 2016, [redacted]

The hackers authenticated to [redacted]

198. [redacted]

[redacted]

199. At the time of the hack, unencrypted PCI was sent to the exposed [redacted] server, where it was encrypted and transmitted to the credit card company. [redacted]

200. [redacted]

201. [redacted]

202. [redacted]

203. [redacted]

204. [redacted]

[redacted]

205. [redacted]

[redacted]

206. [redacted]

[redacted]

207. [redacted]

[redacted]

208. [redacted]

[redacted]

209. [redacted]

[redacted] Hackers obtain password hashes and decrypt them to obtain usable credentials for a network or exploit other security flaws to use the hash instead of the password.

210. [redacted]

211. [redacted]

212. [redacted]

213. On June 21, 2016, the hackers logged into the [redacted] server using the [redacted] account. [redacted]

On the same day, the hackers logged into the [redacted] server using the [redacted] user account. [redacted]

214. [redacted]

215. [redacted]

216. Because Banner did not segment its network, the hackers were able to move laterally across Banner's network and access significantly more information, including Class Member PII and PHI, than they would have if Banner had segmented its network.

217. [redacted]

218. Still on June 21, 2016, the hackers created files on the [redacted] server [redacted] On information and belief, these databases contain PII and PHI of Plaintiffs and Class Members.

219. Because Banner failed to segregate its network, the hackers were able to obtain access to these databases from their point of entry into the network; because Banner failed to restrict access of its accounts to the servers containing PII and PHI, the hackers were able to use the hacked accounts to move freely across the network and to access the databases of sensitive information.

220. [redacted]

221. [redacted]

222. On June 23, 2016, the hackers accessed the Banner database [redacted]

223. Accordingly, on information and belief, the hackers accessed, copied, and removed the PII and PHI of Plaintiffs and Class Members.

224. [redacted]

225. [redacted]

[redacted]

226. [redacted]

227. In all, it took the hackers a total of approximately four days, from June 17 to June 21, 2016, to access PII and PHI on Banner's systems—a very short amount of time, reflecting the ease with which the hackers were able to survey and move laterally within Banner's network. It took an additional two days, until June 23, 2016, to first access the PCI of Banner food and beverage outlet customers. [redacted]

228. [redacted]

229. On June 29, 2016, Banner's IT team was asked to investigate system slowness on various servers. [redacted]

230. [redacted]

231. On or around July 7, 2016, [redacted]

232. [redacted]

233. [redacted] Banner has yet to perform a network wide review and full audit of its systems, though the need for such action was known since at least 2012.

234. [redacted] It is extremely unlikely that the hackers would collect over 22,000 payment cards' worth of PCI without exfiltrating that data multiple times during the two-week period that the scraping was underway. [redacted]

235. [redacted]

236. [redacted]

237. [redacted]

238. Banner waited until August 3, 2016, to publicly announce that the data breach had occurred, and said that all affected individuals would receive a breach notification letter by September 9, 2016.

239. Jeff Williams, co-founder of Contrast Security, queried why it took three weeks for Banner to discover the attack, why it took another week to discover the attack on patient information, and why it took almost a month for Banner to release any information about the breach. He also noted that Banner gave no details regarding how long attackers were in the system before they were discovered.

VI. Banner's Patients, Insurance Plan Members, Plan Beneficiaries, Customers, Providers, and other Employees Were and Will Continue to Be Harmed by Banner's Information-Security Failures and the Resultant Data Breach.

240. Banner's information security failures led directly to the compromise and theft of the PII, PHI, and PCI to which it had been entrusted. This has and will continue to cause harm to Banner's patients, insurance plan members, plan beneficiaries, payment card customers, healthcare providers and other employees.

241. According to Banner, the data breach impacted a total of approximately 3.7 million people. That makes it the ninth largest healthcare data breach of all time, per the OCR of HHS. According to a National Consumers League report, about one in three data breach victims suffer identity fraud and that rate has increased in recent years.[4]

242. Banner acknowledged that the hackers accessed PII and PHI of its patients and insurance plan members, the PII of its plan beneficiaries, providers, and employees, and the PCI of approximately 22,000 customers who used payment cards at 27 Banner food and beverage outlets in point-of-sale transactions.

243. Banner acknowledged that the hackers accessed the servers where Banner stored the PII and PHI of its patients and insurance plan members, including their names, birthdates, addresses, physicians' names, dates of service, claims information, clinical information, health insurance information, and social security numbers.

244. Banner acknowledged that the hackers accessed the data systems holding Banner's providers' PII, including their names, addresses, birthdates, Drug Enforcement Agency numbers, Tax Identification numbers, National Provider Identifiers, and social security numbers.

245. The hackers compromised and accessed Banner server [redacted] The [redacted]

[4] *See* National Consumers League, The Consumer Data Insecurity Report: Examining the Data Breach – Identity Fraud Paradigm in Four Major Metropolitan Areas, http://www.nclnet.org/datainsecurity_report (last visited March 3, 2017).

[redacted]

246. [redacted]

[redacted]

247. [redacted]

[redacted]

248. With respect to the stolen PHI, Banner's patients' and insurance plan members' most sensitive, personal information has been compromised. Rather than continuing to be safeguarded by an ostensibly HIPAA compliant entity, it is in the hands of criminals and likely already has and will continue to make its way into the hands of other criminals. Banner's patients and insurance plan members will never be confident of the privacy and security of that highly personal information again. In addition, the PHI and PII has already and will continue to be used to conduct identity theft, financial fraud, and medical and pharmaceutical fraud. This fraud has already and will continue to cause major financial, medical, and reputational harm.

249. The social security numbers and other corroborating PII exposed through the data breach create an imminent risk of identity fraud for Plaintiffs and the Class

Members. Criminals frequently use stolen social security numbers to create false bank accounts, file fraudulent tax returns, file for unemployment benefits, or apply for a job using a false identity. As the Social Security Administration has warned, identity thieves can use an individual's social security number and good credit score to apply for credit in the name of the victim. This type of fraud can go undetected for years.

250. Because social security numbers, dates of birth, and the like never change, identity thieves often hold onto this information, using it to commit fraud years after free credit monitoring programs expire. Identity theft victims may be denied loans for education, housing, or cars due to negative information in their credit reports resulting from identity fraud.

251. Generally, individuals cannot obtain a new social security number until *after* evidence of ongoing problems caused by misuse already exists. Even then, the Social Security Administration warns that "a new number probably won't solve all [ ] problems . . . and will not guarantee [ ] a fresh start." For some victims of identity theft, "a new number actually creates new problems." In fact, according to Julie Fergerson, chair of the Identity Theft Resource Center, the "credit bureaus and banks are able to link the new number very quickly to the old number, so that old bad information is quickly inherited into the new Social Security number."

252. Those affected by the Banner data breach will thus need to continue spending time and energy undertaking prophylactic measures, including contacting agencies like the Internal Revenue Service, Social Security Administration, and their state tax boards. They will also need to monitor their credit and tax filings for many years. They will have to spend time and money securing their personal information and protecting their identities. They will need to monitor their accounts and credit, and will have to pay for credit monitoring and credit reports. All of this is a direct result of Banner's failure to protect their information.

253. Unfortunately, though identity fraud is a common result from a data breach, it is difficult to uncover. Individuals may not know that their social security numbers

have been used to file for unemployment benefits, for example, until law enforcement becomes involved by notifying the individual's employer of the suspected fraud (which, in turn, may cause adverse consequences at work).

254. Further risk inheres from the exposure of the PCI entrusted to Banner.

[redacted]

255. PCI is typically distributed quickly through private criminal networks or sold on black market web forums on the so-called "Dark Web" to facilitate credit card fraud. The customers whose PCI was compromised face the prospect of paying fees to their banks for new debit and credit cards, paying fees to have the cards shipped faster so that they do not have to wait weeks to make purchases on their accounts, and otherwise dealing with the hassle, inconvenience, and distress of trying to resolve fraudulent charges, obtain replacement payment cards, and correct information in their credit reports. They also face the hassle and inconvenience of resetting autopayment functionality following card replacement, as well as the prospect of late fees in the event a payment is missed due to card cancellation on autopay accounts.

256. The PCI Security Standards Council, referenced above, warns merchants that "[h]ackers want your cardholder data. By obtaining the Primary Account Number (PAN) and sensitive authentication data, a thief can impersonate the cardholder, use the card, and steal the cardholder's identity." The Council further warns that "[t]he security of cardholder data affects everybody" and that "[t]he breach or theft of cardholder data affects the entire payment card ecosystem. Customers['] … credit can be negatively affected—there is enormous personal fallout."

257. Although identity fraud can be hard to uncover, examples have already been reported by individuals whose PII, PHI, and PCI was compromised in the data breach. Examples include:

- complaints of a fraudulent bank account opened in their name, with the bank "verif[ying] that her social security was used in the process";
- "unauthorized applications" for credit at various retailers, including Kohl's, Sunglass Hut, and Guitar Center;
- receiving notice that a Citibank credit card "had been issued for $11,000.00," even though "they did not apply for the card";
- "receiv[ing] a collection call from PayPal for an account he never opened" and being told by PayPal that "his social security number was associated with the account";
- "receiv[ing] a monitoring alert for 2 chase inquiries for applications she did not authorize";
- "receiving two credit cards in the mail that she did not apply for";
- discovering applications of credit where a creditor "confirmed use of his information";
- "receiv[ing] a letter from Capital One advising an application for a credit card was received that she did not authorize";
- "receiv[ing] a credit card from Compass bank that she did not apply for" with verification that "an account was established without her consent";
- receiving an alert for a new account with Discover and two letters from Chase concerning applications for an American Visa Signature card, with verification that the breach victim's "SSN was used for applications and account";
- receiving "a letter that they are needing a cashiers check for a condo he was buying only [he] is not buying a condo";
- and discovering that someone had "filed a fraudulent tax return with the member's information";

- Plaintiff Halpin's experiences of identity fraud including two accounts that were fraudulently opened in her name, and an unauthorized person filing taxes using her social security number; and
- Plaintiff Maryniak's unauthorized account use and attempted use.

258. Individuals whose PHI is compromised in data breaches are also particularly susceptible to tax return fraud. Using stolen PII, cyber criminals file tax returns in the name and social security number of the victim, seeking refunds under the guise of the victim taxpayer. In 2013, according to the Government Accountability Office, the IRS paid an estimated $5.2 billion in tax refunds obtained from identity theft; it prevented an additional $24.2 billion in fraudulent transfers that year. It is estimated that in 2016 there will be $21 billion in losses due to fraudulent tax refunds, and data breaches are large factor contributing to this form of identity theft. The U.S. Treasury Inspector General for Tax Administration has recognized that "[t]he increasing number of data breaches in the private and public sectors means more personal information than ever before is available to unscrupulous individuals." Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected. It can take months or years, as well as significant expense to the victim, to correct the fraud with the IRS.

259. Individuals whose PHI is compromised in data breaches are also at risk of medical identify theft. Medical identity theft is a crime in which a victim's identifying information is used to see a doctor, get prescription drugs, or obtain or make false claims for medical care. <u>According to the Ponemon Institute, medical identity theft impacted 2.3 million people in 2014, up 21 percent over those impacted in 2013. Medical identity theft is lucrative, in part because insurance companies continue to make payments on stolen identities until after the fraud is detected.</u>

260. <u>Medical records obtained through a data breach can thus be worth hundreds of dollars per individual.</u> Bob Gregg, chief executive of ID Experts, explained that "detailed medical records with unique patient identifying numbers can fetch up to $100 per record," compared with $1 to $3 for a record containing a name, address, and social

security number. Another security expert said that, at a black market auction, a patient medical record sold for $251, compared to credit card records selling for thirty-three cents. According to a PricewaterhouseCoopers report, a "complete identity-theft kit containing comprehensive health insurance credentials can be worth hundreds of dollars or even $1,000 each on the black market." Marc Probst, chief information officer of Intermountain Healthcare in Salt Lake City, said his hospital system fends off thousands of attempts to penetrate its network each week. "The only reason to buy that data is so they can fraudulently bill," Probst said.

261. Medical identity theft can also include Medicare Part D fraud. Victims can be fraudulently enrolled into alternate Part D plans to increase sales commissions.

262. Medical identity theft victims spend, on average, $13,500 to resolve problems stemming from medical identity theft, which for many included out-of-pocket costs for healthcare they did not receive in order to regain coverage. Victims of medical identity theft may also lose their healthcare coverage or experience increased premiums. And, studies have shown that a significant percent of medical identity victims are never able to resolve their identity theft.

263. Beyond the serious financial detriments to individuals whose PHI is exposed in a data breach, there are also health risks. According to the President's Identity Theft Task Force, "victims of medical identity theft may have their health endangered by inaccurate entries in their medical records." This inaccurate information may "cause victims to receive improper medical care, have their insurance depleted, become ineligible for health or life insurance, or become disqualified for some jobs." For example, altering one's health information may lead medical professionals to believe a patient has a different blood type. According to Jason Hart, vice president and CTO for data protection for Gemalto, personal information and medical identity theft is "much harder to remediate" than credit card theft. Medical identity fraud may also lower its victims' credit scores.

264. Victims of data breaches involving medical information, such as this, also face imminent risk of health insurance discrimination. Because their medical information becomes contaminated, victims face denial of coverage, improper "redlining," and denial or difficulty obtaining disability or employment benefits. This risk is pervasive and widespread. Indeed, most states maintain government agencies that investigate and combat health insurance discrimination, as does the OCR.

265. According to a 2015 Ponemon Institute study, only ten percent of respondents report "achieving a completely satisfactory conclusion" of the medical identity theft incident. Those who have resolved the crime "spent, on average, more than 200 hours on such activities as working with their insurer or healthcare provider to make sure their personal medical credentials are secured . . . and verifying their personal health information, medical invoices and claims and electronic health records are accurate." Most victims of medical identity theft do not learn about the theft until more than three months after it has occurred. Due to time and energy spent monitoring one's information and correcting false information, medical fraud also takes an emotional toll on its victims.

266. Information exposed in data breaches regarding medical providers is also often used by specialized criminals who impersonate the providers. These criminals can file false claims, alter medical records, and obtain prescription drugs. Affected providers find themselves targets of civil and criminal investigations into healthcare fraud and may have their licenses suspended.

267. Despite the urgent need for affected individuals to begin taking precautions, Banner did not immediately publicize the data breach after discovering it, instead waiting months to deliver letters to those affected. In the letters, Banner offered victims one year of credit monitoring, identity monitoring, and fraud services through Kroll, Inc. That offer quickly expired, and Banner's data breach information website, bannersupports.com, became inaccessible even before the deadline for signing up for Kroll's services.

268. Kroll's offered services were to monitor only one of the three major credit reporting bureaus, TransUnion, leaving unattended sources from the other credit reporting

bureaus from which identity theft can be detected. Individuals had to sign up for the Kroll services online, but many reported that when they visited the website, their security software identified the website as unsecure. As a result, many were "apprehensive" about signing up because they wanted to avoid "any chance of additional exposure by using an unsecure site." Others, including elderly and lower income individuals, did not have computer access and therefore did not sign up for Kroll's services. Still others share an email address with their spouses, and Kroll did not permit them to sign up for two separate credit monitoring accounts.

269. In any event, a single year of services is inadequate. Data thieves often hold stolen data for more than one year before using it to commit identity theft. In fact, they often wait until consumers are less likely to be looking out for fraudulent activities and they get away with waiting because "healthcare data is lifelong." According to Jeff Williams, one year of credit card monitoring is insufficient to protect individuals from misuse of their healthcare data.

270. Many of the data breach victims were minors who received healthcare at Banner's hospitals or who were beneficiaries of adults' employment benefits or health insurance. Identity fraud affects 1.3 million children annually, 50 percent of whom are younger than six years old. Yet Kroll's services are unavailable to those whose data was breached but who are under 18 years old. Relatedly, credit freezes are not available for many data breach victims who are minors. TransUnion only allows such credit freezes in states that reserve that right for minors and their parents or guardians, and applicable fees may apply. Arizona and most other states do not have minor freeze laws on the books. Some states will only allow parents or guardians to request a freeze if the child is 16 or younger. Unlike adults who can take affirmative steps to monitor their credit, minors typically do not have established credit to monitor. Because their credit history leaves no paper trail, and because minors typically do not monitor their credit, they are a target for identity theft. By the time minors can take action to protect their own credit, their credit may be severely damaged from years of misuse.

271. In addition to the Kroll letter, Banner informed its healthcare providers that Kroll does not monitor National Provider Identity ("NPI") numbers, IRS Tax Identification Numbers ("TIN"), or Drug Enforcement Agency ("DEA") numbers. Banner has asked physicians to monitor their own DEA numbers—a number used to track the prescription of dangerous narcotics and other drugs controlled by the U.S. Drug Enforcement Agency. Kroll does nothing to monitor this vitally important PII that, if compromised, could adversely affect a medical providers' ability to practice medicine. Monitoring DEA, NPI, and TIN numbers, as Banner requested, takes time away from a medical providers practice and unnecessarily and unduly interferes with the providers' ability to earn a living.

272. Finally, Banner has not offered to reimburse any costs associated with pursuing preventive measures—even those recommended by the FTC. The FTC recommends taking multiple steps depending upon the circumstances, including placing a fraud alert, requesting a credit freeze, ordering credit reports, creating an identity theft report, and filing a police report. To guard against medical identity theft, individuals should routinely obtain the most recent copies of their medical records and inspect them for discrepancies. In addition, credit bureaus charge approximately $30 to freeze credit reports, which can be avoided only by filing a police report. Banner is aware of these costs, yet continues not to assist with them.

CLASS ACTION ALLEGATIONS

273. Pursuant to Rule 23 of the Federal Rules of Civil Procedure, Plaintiffs bring this action on behalf of themselves and the following proposed Classes defined as follows:

Patient Class: All Banner healthcare patients whose PII and/ or PHI was maintained on Banner's network and who were mailed a breach notification letter from Banner.

Insured Class: All insurance plan members whose PII and/or PHI was maintained on Banner's network and who were mailed a breach notification letter from Banner.

Employee Class: All Banner healthcare service providers and employees whose PII and/or PHI was maintained on Banner's network and who were mailed a breach notification letter from Banner.

Point-of-Sale Class: All individuals who used a payment card at a Banner location, whose PCI was transmitted through Banner's [redacted] server and who were mailed a breach notification letter from Banner.

274. Plaintiffs reserve the right to amend the class definitions and to define any appropriate subclass or subclasses based on additional facts learned through discovery.

275. Excluded from each of the proposed Classes are Banner; any affiliate, parent, or subsidiary of Banner; Banner's officers, directors, legal representatives, successors, and assigns; anyone employed by counsel in this action; any judge presiding over this matter, his or her spouse, and all persons within the third degree of relationship to either of them and the spouse of such persons.

276. **Numerosity**: Banner announced that 3.7 million people were impacted by the breach, and a majority of those people interacted with Banner in Arizona or Colorado and are thus members of the proposed Classes. Banner employs over 50,000 employees and 7,000 physicians and medical staff members and is both Arizona's largest private employer and one of Northern Colorado's largest employers. Banner's revenues from serving patients is approximately $6 billion annually and its revenues from health insurance premiums is approximately $1 billion annually; a majority of those revenue streams derives from patients and insureds in Arizona and Colorado who are members of the proposed Classes.

277. **Commonality and Predominance**: Common questions of law and fact exist as to all proposed Class Members and predominate over questions affecting only individual Class Members. These common questions include whether:

a. Banner was obligated to safeguard Plaintiffs' and the Class Members' PII, PHI, and PCI;

b. Banner breached its obligation to safeguard Plaintiffs' and the Class Members' PII, PHI, and PCI;

c. Banner failed to implement reasonable, industry-standard safeguards for Plaintiffs' and the Class Members' PII, PHI, and PCI;

d. Banner failed to disclose its inability, to adequately safeguard Plaintiffs' and the Class Members' PII, PHI, and PCI;

e. Banner's inadequate information security practices violated federal and state law;

f. Banner's failure to safeguard Plaintiffs' and the Class Members' PII, PHI, and PCI led to a data breach in 2016 during which the security of Plaintiffs' and the Class Members' PII, PHI, and PCI was compromised;

g. Banner's inadequate information security practices have harmed Plaintiffs and the Class Members and have put them at imminent risk of future harm;

h. Banner failed to take reasonable steps to mitigate the effects of the data breach, including by failing to notify Plaintiffs and Class Members about the data breach as soon as practicable after its discovery;

i. Banner should return the money paid by Plaintiffs and Class Members to protect their PII, PHI, or PCI;

j. Plaintiffs and Class Members are entitled to damages, restitution, or some other form of remuneration as a result of Banner's wrongful conduct; and

k. Injunctive or other equitable relief is appropriate to redress Banner's wrongful conduct and, if so, what form it should take.

278. **Typicality**: Plaintiffs' claims are typical of the claims of the members of the Classes. Plaintiffs, like all other members of the Classes, entrusted their PII, PHI, or PCI to Banner, and have sustained damages as a result of Banner's uniform failure to adequately safeguard that information.

279. **Adequacy of Representation**: Plaintiffs are adequate representatives of the proposed classes because neither their nor their counsel's interests conflict with the

interests of the members of the Classes they seek to represent. Plaintiffs have retained counsel competent and experienced in complex class action litigation and will prosecute this action vigorously on Class Members' behalf.

280. **Superiority**: A class action is superior to other available means for the fair and efficient adjudication of this dispute. The injury suffered by each Class Member, while meaningful on an individual basis, is not of such magnitude as to make the prosecution of individual actions against Banner economically feasible. Even if Class Members themselves could afford such individualized litigation, the court system could not. In addition to the burden and expense of managing many actions arising from the data breach, individualized litigation presents a potential for inconsistent or contradictory judgments. Individualized litigation increases the delay and expense to all parties and the court system presented by the legal and factual issues of the case. By contrast, a class action presents far fewer management difficulties and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court.

281. In the alternative, the proposed Classes may be certified because:

a. The prosecution of separate actions by the individual members of the proposed class would create a risk of inconsistent adjudications, which could establish incompatible standards of conduct for Banner;

b. The prosecution of individual actions could result in adjudications, which as a practical matter, would be dispositive of the interests of non-party class members or which would substantially impair their ability to protect their interests; and

c. Banner has acted or refused to act on grounds generally applicable to the proposed Classes, thereby making appropriate final and injunctive relief with respect to the members of the proposed classes as a whole.

FIRST CAUSE OF ACTION
Negligence
(All Plaintiffs on behalf of the proposed Classes)

282. Plaintiffs reallege the paragraphs above as if fully set forth herein.

283. Banner accepted Plaintiffs' and Class Members' nonpublic PII, PHI, and PCI in connection with its agreement to provide healthcare services, insurance plan membership, employment and employment benefits, and food and beverages.

284. Banner not only collected, but maintained, accessed, and utilized this data.

285. Banner owed Plaintiffs and Class Members a duty of reasonable care in the handling, maintenance and security of their PII, PHI, and PCI. This duty included taking reasonable measures to prevent disclosure of the information and reasonable measures to guard the information from cyberattacks.

286. Banner was required to secure and safeguard the PII, PHI, and PCI of Plaintiffs and Class Members, to prevent disclosure of the information, and to guard the information from theft. Banner was further under a duty and had a responsibility to implement a process by which it could detect a breach of its security systems in a reasonably expeditious period of time so that it could respond, remedy, and promptly notify affected individuals in the event of a security breach. Banner was further required to maintain PII, PHI, and PCI as long as necessary and required by law.

287. Banner knew or should have known that the risk in collecting and storing the PII, PHI, and PCI of Plaintiffs and Class Members and of the critical importance of providing adequate security of that information.

288. Banner's duties arise from the common law, the state statutes cited in this Complaint, the Federal Trade Commission Act and the following HIPAA regulations:

a. 45 C.F.R. § 164.306(a)(1) for failing to ensure the confidentiality and integrity of electronic PII and PHI that Banner created, received, and maintained from Plaintiffs and Class Members.

b. 45 C.F.R. § 164.306(a)(2) for failing to protect against reasonably anticipated threats or hazards to the security or integrity of the electronic PII and PHI of Plaintiffs and Class Members;

c. 45 C.F.R. § 164.306(a)(3) for failing to protect against reasonably anticipated uses or disclosures of electronic PHI not permitted under the privacy rules regarding individually identifiable health information;

d. 45 C.F.R. § 164.306(a)(4) for failing to ensure compliance with the HIPAA security standard rules; and

e. 45 C.F.R. § 164.308(a)(1)(i) for failing to implement policies and procedures to prevent, detect, contain and correct security violations.

289. Banner breached its duty of care by failing to secure and safeguard the PII, PHI, and PCI of Plaintiffs and Class Members as detailed in this Complaint. Banner negligently maintained data systems that it knew were vulnerable to a security breach. While it knew or should have known of such vulnerabilities, it wholly failed to rectify them or take steps to safeguard the information in a timely fashion.

290. Plaintiffs and Class Members have suffered harm as a result of Banner's breach of duty. The PII, PHI, and PCI of Plaintiffs and Class Members was exposed, subjecting each Class member to identity theft, credit and bank fraud, social security fraud, tax fraud, medical identity fraud and other varieties of identity fraud.

291. Plaintiffs and Class Members suffered monetary damages and will continue to be injured and incur damages in the future in an effort to both protect themselves and to remedy acts of fraudulent activity. Plaintiffs and Class Members have suffered and such are reasonably likely to suffer: theft of personal health information; costs associated with prevention, detection and litigation of identity theft; costs associated with time spent and productivity loss resulting from addressing the consequences of fraud in any of its myriad form; and damages from the exposure of their PII, PHI, and PCI due to Banner's misconduct and breach.

SECOND CAUSE OF ACTION
Negligence Per Se (HIPAA, the FTC Act)
(All Plaintiffs on behalf of the proposed Classes)

292. Plaintiffs reallege the paragraphs above as if fully set forth herein.

293. Banner required Plaintiffs and Class Members to provide it with confidential and private PII and PHI in order to provide healthcare services, health insurance, or other services to Plaintiffs and Class Members.

294. Based on those requirements and in order to obtain services from Banner, Plaintiffs and Class Members provided Banner with PII and PHI belonging to Plaintiffs and Class Members.

295. Banner collected and stored this information and knew, or should have known, of the risks inherent in collecting and storing the PII and PHI of Plaintiffs and Class Members.

296. Pursuant to HIPAA, 42 U.S.C. § 1302d *et seq.*, Banner had a duty to implement reasonable safeguards to protect Plaintiffs' and Class Members' PII and PHI.

297. Pursuant to the Federal Trade Commission Act, 15 U.S.C. § 45, Banner had a duty to provide fair and adequate computer systems and data security practices in order to safeguard Plaintiffs' and Class Members' PII and PHI.

298. Through its acts and omissions, including those described above, Banner violated its obligations under HIPAA and the Federal Trade Commission Act.

299. Banner's failure to comply with its duties under these acts breached its duty of reasonable care to Plaintiffs and Class Members and constituted negligence per se.

300. Banner's actions were the direct and proximate cause of harm to Plaintiffs and Class Members. But for Banner's actions and failures to act, Plaintiffs and the Class Members would not have been injured and their PII and PHI would have been secure.

301. Plaintiffs' injuries and those of the Class Members were reasonably foreseeable as a result of Banner's breach of its duties to Plaintiffs and Class Members. Banner knew or reasonably should have known that its breach of its duties would put Plaintiffs' and Class Members' PII and PHI at risk and the failure to adequately protect that information would harm Plaintiffs and Class Members.

302. As a direct and proximate result of Banner's breaches of its duties, Plaintiffs and Class Members have suffered harm because, among other things, their PII and PHI

has been exposed, imminently subjecting each Class Member to identity theft, credit and bank fraud, social security fraud, tax fraud, medical identity fraud and other varieties of identity fraud.

303. Plaintiffs and Class Members have suffered monetary damages and/or will incur monetary damages in the future both in an effort to protect themselves and to remedy acts of fraudulent activity. Plaintiffs and Class Members have suffered, and/or face an imminent risk of suffering: the theft of their credit identity and medical identities; costs associated with prevention, detection, and mitigation of identity theft, medical identity theft, and/or fraud; costs associated with time spent and productivity loss resulting from addressing the consequences of, or preventing, fraud in any of its forms; and damages from the unconsented exposure of PII and PHI due to this breach.

THIRD CAUSE OF ACTION
Breach of Contract
(All Plaintiffs on behalf of the proposed Classes)

304. Plaintiffs reallege the paragraphs above as if fully set forth herein.

305. As set forth above, Plaintiffs and those Class Members who received medical care from Banner, were insurance plan members, or were employed by Banner or permitted to act as a Banner healthcare provider, all entered into binding and enforceable contracts with Banner.

306. The contracts between Plaintiffs and Class Members and Banner were supported by consideration in many forms, and Plaintiffs and Class Members performed pursuant to these contracts, including: by paying for healthcare service; paying insurance premiums, contributions, or fees; and performing their duties as Banner employees and healthcare providers.

307. All contracts between Plaintiffs and Class Members and Banner were entered into prior to the June and July 2016 data breach.

308. As a condition of receiving treatment, insurance, employment, or authorization to act as a healthcare provider, Plaintiffs and Class Members provided PII and PHI to Banner.

309. As set forth above, all Plaintiffs and Class Members who received Banner healthcare services entered into contracts with Banner that incorporated, either by express provision or attachment, or incorporation by reference, Banner's then-current privacy policies pertaining to personal and health-related information, including but not limited to the Notice of Privacy Practices set forth at all times on Banner's Privacy Practices for Banner Health webpage.

310. As set forth above, all Plaintiffs and Class Members who were insurance plan members entered into contracts that include, either by express provision or attachment, or incorporation by reference, Banner's then-current privacy policies pertaining to personal health-related information, including but not limited to the Privacy Practices in Banner Plans and Summary Plan Description documents.

311. As set forth above, all Plaintiffs and Class Members who were employed by Banner entered into contracts that include, either by express provision or attachment, or incorporation by reference, Banner's then-current privacy policies pertaining to employees' and health care providers' personally identifiable information, including but not limited to the Employee Handbook and the Banner Workforce Confidentiality Policy.

312. Banner materially breached the terms of its contracts with Plaintiffs and Class Members by violating its commitment to maintain the confidentiality and security of their PII and PHI, and by failing to comply with their own policies and applicable laws, regulations and industry standards for data security and protecting the confidentiality of PII and PHI.

313. As a natural and probable consequence of Banner's breaches, Plaintiffs and Class Members have suffered monetary damages and will incur monetary damages in the future both in an effort to protect themselves and to remedy acts of fraudulent activity. Plaintiffs and Class Members have suffered from, and face an imminent risk of suffering from: incidents of identity and medical fraud; costs associated with prevention, detection, and mitigation of such fraud; costs associated with time spent and productivity loss

resulting from addressing the consequences of, or preventing, such fraud; and damages from the unconsented exposure of PII and PHI due to Banner's breaches.

314. As a result of Banner's breaches of contract, Plaintiffs and Class Members did not receive the full benefit of the bargain, and instead received health insurance and health care services that were less valuable than described in their contracts. Plaintiffs and Class Members, therefore, were damaged in an amount at least equal to the difference in value between that which was promised and Banner's partial, deficient and defective performance.

315. Plaintiffs are entitled to an award of damages, restitution, specific performance, and an award of their reasonable attorneys' fees under A.R.S. § 12-341.01.

FOURTH CAUSE OF ACTION
Breach Of Implied Covenant Of Good Faith And Fair Dealing
(All Plaintiffs on behalf of the proposed Classes)

316. Plaintiffs reallege the paragraphs above as if fully set forth herein.

317. As forth above, Plaintiffs and Class Members entered into binding and enforceable contracts with Banner, which were supported by valid consideration, and Plaintiffs and Class Members performed pursuant to these contracts.

318. Plaintiffs and Class Members entered into those contracts before the June and July 2016 data breach.

319. Plaintiffs and Class Members performed all conditions, covenants, obligations, and promises owed to Banner, including: paying for their healthcare services, paying insurance premiums, contributions, and fees; carrying out their responsibilities as Banner employees and healthcare service providers; and providing Banner the requisite confidential information.

320. Every contract contains an implied covenant of good faith and fair dealing, which requires parties to a contract not to take any actions that would bear adversely on the other party's reasonably expected benefits of the bargain.

321. As set forth above, Banner promised to protect Plaintiffs' and Class Members' PII and PHI. Even if Banner is held not to have breached any express promise

in these contracts, Banner breached the covenant of good faith and fair dealing by failing to take adequate measures to protect the confidentiality of Plaintiffs' and Class Members' PII and PHI, resulting in the June and July 2016 data breach. Banner unreasonably interfered with the contract benefits owed to Plaintiff and Class Members by: compiling and storing Plaintiff and Class Members' data with unreasonable and inadequate cybersecurity protections and by permitting unrestricted access to the PII and PHI entrusted to it.

322. As a natural and probable consequence of Banner's breaches, Plaintiffs and Class Members have suffered monetary damages and will incur monetary damages in the future both in an effort to protect themselves and to remedy acts of fraudulent activity. Plaintiffs and Class Members have suffered from, and face an imminent risk of suffering from: incidents of identity and medical fraud; costs associated with prevention, detection, and mitigation of such fraud; costs associated with time spent and productivity loss resulting from addressing the consequences of, or preventing, such fraud; and damages from the unconsented exposure of PII and PHI due to Banner's breaches.

323. As a result of Banner's breaches of contract, Plaintiffs and Class Members did not receive the full benefit of the bargain, and instead received health insurance and health care services that were less valuable than described in their contracts. Plaintiffs and Class Members, therefore, were damaged in an amount at least equal to the difference in value between that which was promised and Banner's partial, deficient and defective performance.

324. Plaintiffs are entitled to an award of damages, restitution, specific performance, and an award of their reasonable attorneys' fees under A.R.S. § 12-341.01.

FIFTH CAUSE OF ACTION
Breach of Implied Duty to Perform with Reasonable Care
(All Plaintiffs on behalf of the proposed Classes)

325. Plaintiffs reallege the paragraphs above as if fully set forth herein.

326. As forth above, Plaintiffs and Class Members entered into binding and enforceable contracts with Banner, which were supported by valid consideration, and Plaintiffs and Class Members performed pursuant to these contracts.

327. Plaintiffs and Class Members entered into those contracts before the June and July 2016 data breach.

328. Plaintiffs and Class Members performed all conditions, covenants, obligations, and promises owed to Banner, including: paying for their healthcare services, paying insurance premiums, contributions, and fees; carrying out their responsibilities as Banner employees and healthcare service providers; and providing Banner the requisite confidential information.

329. As noted above and throughout, for Banner to meet its contractual obligations, it was necessary for Plaintiffs and Class Members to provide to and share with Banner their PII and PHI and for Banner to hold, use, and store that PII and PHI.

330. The contracts, between Banner, on one hand, and Plaintiffs and Class Members, on the other hand, were an undertaking for consideration, which bestowed a duty upon Banner to perform its contractual obligations competently and with reasonable care.

331. This required Banner to use reasonable care in safeguarding the PII and PHI with which it was entrusted, in particular given the sensitivity and value of the information, governing law and industry custom, and the known threat posed by cybercriminals. This obligation is not only express (through Banner's own internal documents, contracts and policies), but implied through Banner's course of dealing with Plaintiffs and Class Members, industry practice, and state and federal law.

332. Banner failed to perform its obligations competently and with reasonable care because it failed to take reasonable and adequate measures to protect the confidentiality of Plaintiffs' and Class Members' PII and PHI, resulting in the June and July 2016 data breach. Banner compiled, stored, and used Plaintiffs' and Class Members'

data using unreasonable and inadequate cybersecurity protections and permitted unrestricted access to the PII and PHI entrusted to it.

333. As a natural and probable consequence of Banner's breaches, Plaintiffs and Class Members have suffered monetary damages and will incur monetary damages in the future both in an effort to protect themselves and to remedy acts of fraudulent activity. Plaintiffs and Class Members have suffered from, and face an imminent risk of suffering from: incidents of identity and medical fraud; costs associated with prevention, detection, and mitigation of such fraud; costs associated with time spent and productivity loss resulting from addressing the consequences of, or preventing, such fraud; and damages from the unconsented exposure of PII and PHI due to Banner's breaches.

334. As a result of Banner's breaches of contract, Plaintiffs and Class Members did not receive the full benefit of the bargain, and instead received health insurance and health care services that were less valuable than described in their contracts. Plaintiffs and Class Members, therefore, were damaged in an amount at least equal to the difference in value between that which was promised and Banner's partial, deficient and defective performance.

335. Plaintiffs are entitled to an award of damages, restitution, specific performance, and an award of their reasonable attorneys' fees under A.R.S. § 12-341.01.

SIXTH CAUSE OF ACTION
Unjust Enrichment
(All Plaintiffs on behalf of the proposed Classes)

336. Plaintiffs reallege the paragraphs above as if fully set forth herein.

337. Plaintiffs and Class Members conferred a monetary benefit on Banner in the form of monies paid for the purchase of insurance plan premiums and healthcare services.

338. Banner appreciated or had knowledge of the benefits conferred upon it by Plaintiffs and Class Members.

339. The monies for insurance plan premiums and healthcare services that Plaintiffs and Class Members paid (directly or indirectly) to Banner were supposed to be

used by Banner, in part, to pay for the administrative costs of reasonable data privacy and security practices and procedures.

340. As a result of Banner's conduct, Plaintiffs and Class Members suffered actual damages in an amount equal to the difference in value between insurance plan and healthcare services with the reasonable data privacy and security practices that Plaintiffs and Class Members paid for, and the inadequate insurance plan and healthcare services without reasonable data privacy and security practices and procedures that they received.

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

342. Banner should be compelled to disgorge into a common fund for the benefit of Plaintiffs and Class Members all unlawful or inequitable proceeds received by it.

SEVENTH CAUSE OF ACTION
Violation of the Arizona Consumer Fraud Act, A.R.S. § 44-1521, *et seq.*
(All Plaintiffs on behalf of the proposed Classes)

343. Plaintiffs reallege the paragraphs above as if fully set forth herein.

344. Defendant Banner sold Plaintiffs and other Class Members "merchandise" as that term as defined by A.R.S. § 44-1521, in the form of services, including health and insurance services, as well as the sale of objects, wares, goods, and commodities at outlets where Banner accepted payment cards in point-of-sale transactions.

345. Section 44-1522 of the Arizona Consumer Fraud Act provides:

> The act, use or employment by any person of any deception, deceptive or unfair act or practice, fraud, false pretense, false promise, misrepresentation, or concealment, suppression or omission of any material fact with intent that others rely on such concealment, suppression or omission, in connection with the sale or advertisement of any merchandise whether or not any person has in fact been misled, deceived or damaged thereby.

See A.R.S. § 44-1522(A).

346. Defendant Banner used deception, used a deceptive act or practice, and fraudulently omitted and concealed material facts in connection with the sale or advertisement of that merchandise in violation of A.R.S. §44-1522(A).

347. Banner omitted and concealed material facts, which it knew about and had the duty to disclose—namely, Banner's inadequate privacy and security protections for Plaintiffs' and other proposed Class Members' PII, PHI, and PCI. Banner omitted and concealed those material facts even though in equity and good conscience they should have been disclosed and did so with the intent that others would rely on the omission, suppression, and concealment.

348. The concealed facts are material in that they are logically related to the transactions at issue and rationally significant to the parties in view of the nature and circumstances of those transactions.

349. Plaintiffs do not allege any claims based on any affirmative misrepresentations by Banner; rather Plaintiffs allege that Banner omitted, failed to disclose and concealed material facts and information as alleged herein, despite its duty to do so.

350. Banner knew or should have known that its computer systems and data security practices were inadequate to safeguard Plaintiffs' and the other proposed Class Members' PII, PHI, and PCI, and that the risk of a data breach or theft was highly likely. Banner's actions in engaging in these deceptive acts and practices were negligent, knowing and willful, and wanton and reckless with respect to the rights of Plaintiffs and the Class Members.

351. Plaintiffs and the Class Members were ignorant of the truth and relied on the concealed facts and incurred damages as a consequent and proximate result.

352. Plaintiffs and the Class Members seek all available relief under A.R.S. § 4421, *et. seq.*, including, but not limited to, compensatory damages, punitive damages, injunctive relief, and attorneys' fees and costs.

EIGHTH CAUSE OF ACTION
Breach of an Implied Contractual Term
(All Plaintiffs on behalf of the proposed Patient, Insured, and Employee Classes)

353. Plaintiffs reallege the paragraphs above as if fully set forth herein.

354. As set forth above, Plaintiffs and those Class Members who received medical care from Banner, were insurance plan members, or were employed by Banner, or permitted to act as a Banner healthcare provider, all entered into binding and enforceable contracts with Banner.

355. The contracts between Plaintiffs and Class Members and Banner were supported by consideration in many forms, and Plaintiffs and Class Members performed pursuant to these contracts, including but not limited to: by paying for healthcare service; paying insurance premiums, contributions, or fees; and performing their duties as Banner employees and healthcare providers.

356. All contracts between Plaintiffs and Class Members and Banner subject of this claim were entered into prior to the June and July 2016 data breach.

357. As a condition to those contracts, Plaintiffs and Class Members provided PII and PHI to Banner.

358. Banner accepted Plaintiffs and Class Members PII and PHI and by its acceptance, conduct, and statements, implicitly promised and agreed to safeguard Plaintiffs' and Class Members' PII and PHI.

359. Banner's promises and agreements to safeguard Plaintiffs' and Class Members' PII and PHI, though not expressed, were implied terms under the foregoing contracts that, in turn, obligated Banner to secure and safeguard Plaintiffs' and Class Members' PII and PHI.

360. As described throughout, Banner did not take the steps it promised to take – nor the steps a reasonable person would have taken under the circumstances – to safeguard Plaintiffs' and Class Members' PII and PHI. As a result, Banner breached the implied terms in each of its foregoing contracts requiring it to safeguard that information.

361. As a natural and probable consequence of Banner's breaches, Plaintiffs and Class Members have suffered monetary damages and will incur monetary damages in the future both in an effort to protect themselves and to remedy acts of fraudulent activity. Plaintiffs and Class Members have suffered from, and face an imminent risk of suffering from: incidents of identity and medical fraud; costs associated with prevention, detection, and mitigation of such fraud; costs associated with time spent and productivity loss resulting from addressing the consequences of, or preventing, such fraud; and damages from the unconsented exposure of PII and PHI due to Banner's breaches.

362. As a result of Banner's breaches of contract, Plaintiffs and Class Members did not receive the full benefit of the bargain, and instead received health insurance and health care services that were less valuable than described in their contracts. Plaintiffs and Class Members, therefore, were damaged in an amount at least equal to the difference in value between that which was promised and Banner's partial, deficient, and defective performance.

363. Plaintiffs are entitled to an award of damages, restitution, specific performance, and an award of their reasonable attorneys' fees under A.R.S. § 12-341.01.

NINTH CAUSE OF ACTION
Promissory Estoppel
(All Plaintiffs on behalf of the proposed Patient, Insured, and Employee Classes)

364. Plaintiffs reallege the paragraphs above as if fully set forth herein.

365. Banner made numerous representations to Plaintiffs and Class Members, including but not limited to those set forth in paragraphs 91 through 111 above, that it would protect and maintain the security and confidentiality of their PII and PHI.

366. Banner made these representations for the express purpose of inducing Plaintiffs and Class Members to enter into relationships with them for the provision of healthcare services and other services. It was reasonably foreseeable that Plaintiffs and Class Members would rely on these promises in part because Banner made so many representations to protect the confidentiality of the information but also because the type of information at issue is almost never disclosed by owners without assurances of

protection due to the dramatic harm that can befall them if the information gets in the wrong hands.

367. These representations were material to Plaintiffs and Class Members. Plaintiffs and Class Members justifiably and expressly relied on these representations by supplying Banner with their PII and PHI. It was reasonable for Plaintiffs and Class Members to rely on Banner's representations because Banner is required to protect PII and PHI under federal law and, in the absence of such promises and representations, to protect their confidential PII, PHI, PCI, no reasonable person would have provided their PII and PHI to Banner.

368. As a result of Banner's failure to protect their PII and PHI, Plaintiffs and Class Members relied on Banner's promises and representations to their detriment. By virtue of Banner's failure to protect the information and the subsequent breach of its systems by cyber criminals, the PII and PHI of Plaintiffs and the Class Members has been stolen, subjecting them to credit theft, identity theft, and medical-identity theft. Additionally, Plaintiffs and Class Members have incurred or will incur direct costs associated with protecting themselves from such criminal activities and restoring harm caused by them.

369. Under the circumstances, it would be unjust to allow Banner not to abide by its promises and representations to protect and secure the PII and PHI of Plaintiffs and Class Members. Such injustice can only be avoided by holding Banner to its promises and enforcement of Banner's representations and promises to protect and secure the PII and PHI of Plaintiffs and Class Members.

370. By virtue of its actions, including but not limited to those set forth above, Banner breached its promises and representations to Plaintiffs and Class Members to protect their PII and PHI.

371. As a direct and proximate result of Banner's breach of its promises and representations, Plaintiffs and Class Members have suffered actual damages resulting

from the theft of their PII and PHI and remain at imminent risk of suffering additional damages in the future by credit theft, identity theft, and medical-identity theft.

372. As a direct and proximate result of Banner's breach of its promises and representations, Plaintiffs and Class Members are entitled to damages against Banner in an amount to be determined at trial.

PRAYER FOR RELIEF

Plaintiffs, on behalf of themselves and all others similarly situated, request the Court enter judgment against Defendant, as follows:

A. An order certifying the proposed Classes and appointing the undersigned as Class Counsel;

B. An order awarding Plaintiffs and the Class Members relief, including actual and statutory damages, as well as appropriate equitable and injunctive relief;

C. An award of restitution, damages, and any other monetary relief needed to appropriately compensate Plaintiffs and Class Members;

D. An award of punitive damages;

E. An award of attorneys' fees and reimbursement of litigation costs, as provided by law;

F. An award of pre-judgment and post-judgment interest, as provided by law;

G. Leave to amend this Complaint to conform to the evidence produced at trial; and

H. Any other favorable relief as may be available and appropriate under law or at equity.

DEMAND FOR JURY TRIAL

Pursuant to Federal Rule of Civil Procedure 38(b), Plaintiffs demand a trial by jury of any and all issues in this action so triable of right.

RESPECTFULLY SUBMITTED and dated this 16th day of January 2018.

GALLAGHER & KENNEDY, P.A.

By: *s/ Paul L. Stoller*
Paul L. Stoller
Lincoln Combs
2575 E. Camelback Road, Suite 1100
Phoenix, Arizona 85016-9225

Andrew S. Friedman
William F. King
BONNETT FAIRBOURN FRIEDMAN & BALINT, P.C.
2325 E. Camelback Road, Suite 300
Phoenix, Arizona 85016

Interim Co-Lead Class Counsel

Eric H. Gibbs (pro hac vice)
David Stein (pro hac vice)
Amanda M. Karl (pro hac vice)
GIRARD GIBBS LLP
505 14th Street, Suite 1110
Oakland, California 94612
ehg@classlawgroup.com
ds@classlawgroup.com
amk@classlawgroup.com

Robert B. Carey (011186)
Leonard W. Aragon (020977)
Michella A. Kras (022324)
HAGENS BERMAN SOBOL SHAPIRO LLP
11 West Jefferson Street, Suite 1000
Phoenix, Arizona 85003
Telephone: (602) 840-5900
rob@hbsslaw.com
leonard@hbsslaw.com
michellak@hbslaw.com

Executive Committee

CERTIFICATE OF SERVICE

I hereby certify that on, January 16, 2018, I electronically transmitted the attached document to the Clerk's Office using the CM/ECF System for filing and transmittal of a Notice of Electronic Filing.

s/Deborah Yanazzo
Deborah Yanazzo