

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

6 Andrew S. Friedman (005425)
William F. King (023941)
7 **BONNETT FAIRBOURN FRIEDMAN**
& BALINT, P.C.
8 2325 E. Camelback Road #300
Phoenix, Arizona 85016
9 Telephone: (602) 274-1100
afriedman@bffb.com
10 bking@bffb.com

11 *Interim Co-Lead Class Counsel*

12 [Additional Counsel on Signature Page]

13 UNITED STATES DISTRICT COURT
14 DISTRICT OF ARIZONA

15
16
17 IN RE BANNER HEALTH DATA
18 BREACH LITIGATION

16 Case No. 2:16-cv-02696-PHX-SRB
REDACTED
17 **PLAINTIFFS' CONSOLIDATED**
18 **AMENDED CLASS ACTION**
19 **COMPLAINT**
20 **DEMAND FOR JURY TRIAL**

21
22
23
24
25
26
27
28

TABLE OF CONTENTS

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

INTRODUCTION 1

PARTIES 4

I. Plaintiffs 4

 A. Howard Chen 4

 B. Betty Clayton 6

 C. Stacey Halpin 7

 D. Kim Maryniak 8

 E. Summer Sadira 9

 F. Stan Griep 10

II. Defendant 11

JURISDICTION AND VENUE 11

FACTS 11

I. Banner Collects, Stores, and Accesses Sensitive Personal Information. 11

II. Banner Was Obligated to Safeguard the PII, PHI, and PCI Entrusted to It. 14

 A. Banner’s Obligations under Federal and State Law to Safeguard PII, PHI, and PCI. 14

 B. Banner’s Promises to Safeguard PII, PHI, and PCI..... 18

 C. Banner’s Obligations Under Industry Guidelines and Standards. 23

 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..... 29

III. Banner Knew Its Data Systems Were at High Risk of Cyber Attack. 30

IV. Banner Knew Its Information Security Was Inadequate. 34

V. Hackers Exploit Banner’s Inadequate Information Security in Data Breach. 47

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. 56

CLASS ACTION ALLEGATIONS 66

FIRST CAUSE OF ACTION Negligence (All Plaintiffs on behalf of the proposed Classes) 69

SECOND CAUSE OF ACTION Negligence Per Se (HIPAA, the FTC Act) All Plaintiffs on behalf of the proposed Classes)..... 71

THIRD CAUSE OF ACTION Breach of Contract (All Plaintiffs on behalf of the proposed Classes) 72

FOURTH CAUSE OF ACTION Breach Of Implied Covenant Of Good Faith And Fair Dealing (All Plaintiffs on behalf of the proposed Classes) 74

FIFTH CAUSE OF ACTION Breach if Implied Duty to Perform with Reasonable Care (All Plaintiffs on behalf of the proposed Classes) 76

SIXTH CAUSE OF ACTION Unjust Enrichment (All Plaintiffs on behalf of the proposed Classes) 78

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

SEVENTH CAUSE OF ACTION Violation of the Arizona Consumer Fraud Act,
Ariz. Rev. Stat. Ann. § 44-1521, *et seq.*
(All Plaintiffs on behalf of the proposed Classes) 79
PRAYER FOR RELIEF 80

1 Plaintiffs Howard Chen, Betty Clayton, Stacey Halpin, Kim Maryniak, Summer
2 Sadira, and Stan Griep, on behalf of themselves and all others similarly situated, allege the
3 following against Defendant Banner Health:

4 **INTRODUCTION**

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

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

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

27 

1 [REDACTED]
2 [REDACTED]
3 4. [REDACTED]
4 [REDACTED]
5 [REDACTED]
6 [REDACTED]
7 [REDACTED]
8 [REDACTED]
9 [REDACTED]
10 [REDACTED]
11 [REDACTED]
12 [REDACTED]
13 [REDACTED]

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

22 6. In June 2016, hackers took advantage of Banner’s many information
23 security failings. [REDACTED]
24 [REDACTED]
25 [REDACTED]
26 [REDACTED]

27 Moreover, although there was no legitimate reason for having its PCI system devices
28 connected to databases that maintain patient, member, and provider PHI and PII, Banner

1 had failed to segregate its systems and instead left the PCI server connected through its
2 enterprise network to its most sensitive and important information—the PII and PHI of
3 Plaintiffs and the Class Members. As a result of this utter lack of network segmentation,
4 the hackers were next able to move laterally through Banner’s enterprise network to
5 access and copy the PHI and PII in those databases. The hackers’ lateral movement
6 through Banner’s systems was rapid, with the hackers taking advantage of Banner’s
7 failure to implement network segmentation and access controls, among other things. Less
8 than one week after first accessing Banner’s network, the hackers accessed and copied
9 large amounts of PII, PHI, and PCI. They then transmitted the data to a location outside
10 Banner’s network and securely deleted many of the files they had created in order to cover
11 their tracks and obfuscate the extent of the breach. It was not until two weeks after the
12 hackers first entered Banner’s network that Banner suspected an infiltration, [REDACTED]

13 [REDACTED]
14 [REDACTED]

15 7. The hackers succeeded in obtaining names, addresses, dates of birth, social
16 security numbers, provider information, medical histories, and more. In other words, they
17 acquired all that is needed to engage in identity theft and medical fraud of nearly four
18 million people. This is already happening. The cybercriminal group that Banner’s
19 forensic examiner identified as the culprit is known in the information security community
20 as a [REDACTED] meaning their goal in acquiring PII, PHI, and
21 PCI is to monetize it. It is therefore assured that the data they stole either has already or
22 will soon make it to criminals determined to engage in identity theft, medical fraud, and
23 the like. The four million victims of the data breach thus face a variety of present,
24 imminent, and long-lasting risks. Already, many have been victimized by fraud
25 attempts—and they may be the fortunate ones because identity theft and medical fraud are
26 often discovered, if at all, only after severe credit harm, false account charges or other
27 damages have already occurred.

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

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

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

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

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

28

1 B. Betty Clayton

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

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

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

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

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

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

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

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

1 C. Stacey Halpin

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

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

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

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

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

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

21 32. On or about August 3, 2016, Ms. Halpin, her husband, and her son received
22 a letter from Banner informing her that her PII and PHI may have been compromised as a
23 result of the data breach. After receiving the letter, Ms. Halpin enrolled in the one-year
24 credit monitoring service offered through Kroll.

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

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

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

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

12 D. Kim Maryniak

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

14 38. Ms. Maryniak is currently employed as the Director of Professional Practice
15 at Banner Thunderbird Medical Center, a Banner facility, and has worked there since
16 2015. As a part of her employment, Ms. Maryniak had an employee contract with
17 Banner. Pursuant to that contract, Banner demanded, collected, and received Ms.
18 Maryniak's PII, which Banner maintained in its data systems.

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

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

27 41. Finally, during her time at Banner Thunderbird, Ms. Maryniak purchased
28 food and beverages at the facility's cafeteria using her personal credit card. As part of

1 that transaction, Banner collected and received Ms. Maryniak's payment card information,
2 which Banner maintained in its data systems.

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

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

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

17 E. Summer Sadira

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

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

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

26 48. On or about August 3, 2016, Ms. Sadira received a letter from Banner
27 informing her that her PII and PHI may have been compromised as a result of the data
28 breach. Due to Ms. Sadira's enrollment in Colorado's Address Confidentiality Program,

1 Ms. Sadira did not feel safe by providing Banner with additional information to register
2 with Kroll credit monitoring. Due to the breach, Ms. Sadira's real address is in the public
3 domain, thwarting the purpose of the Address Confidentiality Program, and potentially
4 endangering her and her family.

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

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

15 F. Stan Griep

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

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

20 53. During Mr. Griep's stay at McKee Medical Center, his debit card, which he
21 holds jointly with his wife, was used to purchase food and beverages at the facility's
22 cafeteria. As part of that transaction, Banner collected and received Mr. Griep's PCI,
23 which Banner maintains in its data systems.

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

28

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

7 **II. Defendant**

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

10 **JURISDICTION AND VENUE**

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

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

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

22 **FACTS**

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

24 60. Banner is a Phoenix-based health system with annual revenue of
25 approximately \$7 billion. Banner and its subsidiaries own, control, and lease hospitals,
26 clinics, nursing homes, clinical laboratories, ambulatory surgery centers, home health
27 agencies, a captive insurance company, a foundation, an accountable healthcare
28 organization, a Medicaid-managed health plan and related Medicare Advantage health

1 plan, and other healthcare-related organizations. Banner also holds a 51 percent
2 controlling interest in Sonora Quest Laboratories and a 50 percent non-controlling interest
3 in Veritage LLC. Banner Health includes Banner Pharmacy Services, a network of
4 clinical pharmacists, retail pharmacies, home delivery pharmacies, and specialty care
5 pharmacies.

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

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

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

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

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

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

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

18 68. Banner is also a health insurance provider, with approximately one billion
19 dollars in annual insurance revenue. Banner insureds provide PII and PHI to Banner,
20 including names, addresses, phone numbers, dates of birth, social security numbers,
21 financial information, health and pharmaceutical histories, and detailed treatment
22 information. Banner also receives PII for plan beneficiaries.

23 69. Banner operates food and beverage outlets at many of its locations. People
24 who make purchases at those outlets often do so using credit and debit cards. Using such
25 payment methods, customers provide Banner with sensitive PCI, including information
26 from driver’s licenses and ID cards and what is known as “Track 1” and “Track 2” data.
27 These tracks correspond to the horizontal location of the data within the magnetic strips
28 on standard credit cards and include the credit card account number, credit card type,

1 account holder name, expiration date, service code, and “discretionary” data such as the
2 PIN and card verification value or verification code, which is the anti-fraud security
3 feature used in “card not present” transactions and appears on most major credit and debit
4 cards in the form of a three- or four-digit code.

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

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

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

14 71. HIPAA’s Privacy Rule, otherwise known as “Standards for Privacy of
15 Individually Identifiable Health Information,” establishes national standards for the
16 protection of health information.

17 72. HIPAA’s Security Rule, otherwise known as “Security Standards for the
18 Protection of Electronic Protected Health Information,” establishes national security
19 standards for the protection of health information that is held or transferred in electronic
20 form.

21 73. HIPAA limits the permissible uses of “protected health information” and
22 prohibits the unauthorized disclosure of “protected health information.” 45 C.F.R. §
23 164.502. HIPAA requires that covered entities implement appropriate safeguards for this
24 information. *See* 45 C.F.R. § 164.530(c)(1).

25 74. During the relevant time period, HIPAA obligated Banner to implement
26 technical policies and procedures for electronic information systems that maintain
27 electronic protected health information so that such systems were accessible only to those
28

1 persons or software programs that had been granted access rights. *See* 45 C.F.R. §
2 164.312(a)(1).

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

6 76. During the relevant time period, HIPAA also obligated Banner to implement
7 policies and procedures to prevent, detect, contain, and correct security violations, *see* 45
8 C.F.R. § 164.306(a)(1), and to protect against uses or disclosures of electronic protected
9 health information that are reasonably anticipated but not permitted by the privacy rules,
10 *see* 45 C.F.R. § 164.306(a)(3).

11 77. During the relevant time period, HIPAA obligated Banner to ensure that its
12 workforce complied with HIPAA security standard rules, *see* 45 C.F.R. § 164.306(a)(4),
13 to effectively train its workforce on the policies and procedures with respect to protected
14 health information, as necessary and appropriate for those individuals to carry out their
15 functions and maintain the security of protected health information, 45 C.F.R.
16 § 164.530(b)(1).

17 78. The Office for Civil Rights (“OCR”), within the Department of Health and
18 Human Services (“HHS”), issues guidance to assist HIPAA-covered entities.¹ For
19 example, the guidance regarding Risk Analysis clarifies the expectations of organizations
20 required to meet the Security Rule requirements, including by providing information on
21 risk analysis requirements, elements of risk analysis, and a list of resources for covered
22 entities to access.² The list of resources includes a link to guidelines set by the National
23 Institute of Standards and Technology (“NIST”), which OCR says “represent the industry
24 standard for good business practices with respect to standards for securing e-PHI.”

25 ¹ *See* US Department of Health & Human Services, Security Rule Guidance,
26 <http://www.hhs.gov/hipaa/for-professionals/security/guidance/index.html> (last visited
27 February 19, 2017).

28 ² *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](http://www.hhs.gov/hipaa/for-professionals/security/guidance/final-guidance-risk-analysis/index.html) (last visited February 19, 2017).

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

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

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

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

- 15 a. Alaska Stat. §§ 21.07.040 and 18.23.100 required Banner to treat medical
16 and financial information as confidential and required it to protect medical
17 records from unauthorized access;
- 18 b. A.R.S. §§ 36-509 and 36-2221(D) required Banner to keep medical records
19 and information confidential;
- 20 c. Cal. Civ. Code § 1798.81.5(b) and Cal. Health & Safety Code § 1280.18 (a)
21 required Banner to implement and maintain reasonable security procedures
22 and to protect and safeguard PII and PHI from unauthorized access;
- 23 d. Neb. Rev. Stat. §§ 44-4110.01, 44-4725, 44-7210, 44-4725, 44-32, 172, 38-
24 1225, and 44-901 *et seq.* required Banner to maintain the confidentiality of
25 PII and PHI; and
- 26 e. Nev. Rev. Stat. § 439.590 required Banner to maintain the confidentiality of
27 PHI.

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

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

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

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

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

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

28

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

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

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

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

13 92. Banner provides its patients and insureds with a notice of privacy practices
14 and other privacy statements. As discussed below, Banner also dedicates a section of its
15 website to explaining its privacy and data collection policies. This is consistent with the
16 National Association of Insurance Commissioners Roadmap for Cybersecurity Consumer
17 Protections, which tells consumers to "[e]xpect insurance companies/agencies to have a
18 privacy policy posted on their websites and available in hard copy, if you ask. The
19 privacy policy should explain what personal information they collect, what choices
20 consumers have about their data, how consumers can see and change/correct their data if
21 needed, how the data is stored/protected, and what consumers can do if the
22 company/agency does not follow its privacy policy."

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

26 94. Banner's website contains a "Privacy Practices for Banner Health" page that
27 states: "Banner is committed to protecting the confidentiality of information about you,
28 and is required by law to do so. This notice describes how we may use information about

1 you within Banner and how we may disclose it to others outside Banner. This notice also
2 describes the rights you have concerning your own health information. Please review it
3 carefully and let us know if you have questions.”

4 95. The language quoted in the preceding paragraph, including that “Banner is
5 committed to protecting the confidentiality of information about you, and is required by
6 law to do so,” is repeated within Banner’s Notice of Privacy Practices, which is linked on
7 the same webpage.

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

15 97. The Notice of Privacy Practices states that it “applies to Banner facilities
16 and its personnel, volunteers, students, and trainees” as well as “to other health care
17 providers that come to the facility to care for patients, such as physicians, physician
18 assistants, therapists, emergency services providers, medical transportation companies,
19 medical equipment suppliers, and other health care providers not employed by Banner
20 unless these health care providers give you their own Notice of Privacy Practices.” It also
21 states that “Banner is required by law to give you this Notice and to follow terms of the
22 Notice that is currently in effect.”

23 98. The Notice of Privacy Practices lists a limited set of situations in which
24 personal information can be disclosed, including for research, operational, public safety,
25 and other express reasons. According to the policy, “[o]ther uses and disclosures not
26 described in this Notice will be made only with your written authorization...” On
27 information and belief, Banner maintained and promulgated prior versions of this
28 confidentiality notice beginning at least as early as 1996, after HIPAA was enacted, and

1 each such version of the notice contained a similar commitment to protect the PII and PHI
2 of patients, healthcare plan members, and beneficiaries.

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

9 100. Banner’s Condition of Admission and Treatment form also contains an
10 acknowledgment that the patient or representative was required to initial: “I acknowledge
11 receipt of or I have personally received and decline another copy of the: Notice of Privacy
12 Practices for Banner.”

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

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

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

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

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

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

13 103. Banner also provides a Summary Plan Description booklet to its insureds.
14 The booklet contains, among other things, a section entitled “Privacy of Personal Health
15 Information.” That section states:

16 Banner, as Plan sponsor, is committed to protecting your private and
17 personal health information. Banner has and will continue to enter into
18 agreements with service providers, referred to as ‘business associates,’ that
19 contractually protect your personal health information under the same
20 guidelines as those used by Banner. Banner will not disclose your personal
21 health information without your prior written consent or authorization,
22 except as necessary for your treatment, payment for services recorded,
23 health care operations or as otherwise permitted by law. Additionally, you
24 have the right to access and review your own personal health information in
25 accordance with procedures established by Banner and presented in the
26 Notice of Privacy Practices issued separately.

27 The booklet also states that it

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

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

37 104. In its internal policies, Banner has acknowledged “confidentiality is vital to
38 effective credentialing, peer review and quality assessment/improvement activities,” and

1 that “any breach of the confidentiality of ... credentialing” constitutes a failure to meet
2 certain professional and ethical standards.

3 105. Banner publishes an Employee Handbook, which it provides to its
4 employees.

5 106. The Employee Handbook states:

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

13 107. The Employee Handbook also states:

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

19 108. The Employee Handbook is based on and expressly references internal
20 policies and procedures that govern the conduct of both Banner and its employees. One
21 such policy is the Banner Workforce Confidentiality Policy. That policy states its purpose
22 is to “protect confidential information,” and it states “Banner has a legal and ethical
23 responsibility to safeguard confidential information. Banner will comply with all laws
24 and regulations relating to confidentiality and will protect oral, paper, and electronic
25 confidential information.” The same policy states that it “[a]pplies to all Banner
26 workforce including employees, professional and medical staff, volunteers and students,”
27 and repeats some of the Employee Handbook language quoted above, including “Banner’s
28

1 obligation to protect confidential information is so important that every member of Banner
2 must agree to honor privacy and confidentiality during and beyond employment.”

3 109. The Employee Handbook and incorporated policies form part of the contract
4 between Banner and all of Banner’s employees.

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

16 C. Banner’s Obligations Under Industry Guidelines and Standards.

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

- 24 a. Principle 2: “Confidential and/or personally identifiable consumer
25 information data that is collected, stored and transferred inside or outside of
26 an insurer’s, insurance producer’s or other regulated entity’s network should
27 be appropriately safeguarded.”
28

- 1 b. Principle 8: “Insurers ... should take appropriate steps to ensure that third
2 parties and service providers have controls in place to protect personally
3 identifiable information.”
- 4 c. Principle 9: “Cybersecurity risks should be incorporated and addressed as
5 part of an insurer’s ... enterprise risk management (ERM) process.
6 Cybersecurity transcends the information technology department and must
7 include all facets of an organization.”
- 8 d. Principle 10: “Information technology internal audit findings that present a
9 material risk to an insurer should be reviewed with the insurer’s board of
10 directors or appropriate committee thereof.”
- 11 e. Principle 11: “It is essential for insurers ... to use an information-sharing
12 and analysis organization (ISAO) to share information and stay informed
13 regarding emerging threats or vulnerabilities, as well as physical threat
14 intelligence analysis and sharing.”
- 15 f. Principle 12: “Periodic and timely training, paired with an assessment, for
16 employees of insurers... regarding cybersecurity issues is essential.”

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

26 113. The Council has warned merchants that the account number, cardholder
27 name, expiration date, card verification value, and other data on Tracks 1 and 2 are
28 “sensitive cardholder data”; that the data on Tracks 1 and 2 “must never be stored”; and

1 that merchants must have “a good business reason” for storing any of the other sensitive
2 cardholder data, in which case “that data must be protected.” The Council further
3 instructs merchants to “secure cardholder data where it is captured at the point of sale and
4 as it flows into the payment system. The best step you can take is to not store any
5 cardholder data. This includes protecting ... [p]oint of sale systems, ... networks ...,
6 [and p]ayment card data storage and transmission.”

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

11 115. According to the Council, “[m]ost aspects of the PCI DSS are already a
12 common best practice for security.” Research conducted by Verizon from 2011 through
13 2013 found that organizations that suffered a data breach were less likely to have been
14 compliant with PCI DSS than other organizations.

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

20 117. The PCI DSS includes twelve requirements that specify the framework for a
21 secure payments environment as follows:
22
23
24
25
26
27
28

PCI Data Security Standard – High Level Overview

Build and Maintain a Secure Network and Systems	<ol style="list-style-type: none"> 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	<ol style="list-style-type: none"> 3. Protect stored cardholder data 4. Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	<ol style="list-style-type: none"> 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	<ol style="list-style-type: none"> 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	<ol style="list-style-type: none"> 10. Track and monitor all access to network resources and cardholder data 11. Regularly test security systems and processes
Maintain an Information Security Policy	<ol style="list-style-type: none"> 12. Maintain a policy that addresses information security for all personnel

118. 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.

119. 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

1 that restricts access based on a user’s need to know, and is set to ‘deny all’ unless
2 specifically allowed,” because “[w]ithout a mechanism to restrict access based on user’s
3 need to know, a user may unknowingly be granted access to cardholder data.
4 Additionally, a default ‘deny-all’ setting ensures no one is granted access until and unless
5 a rule is established specifically granting such access.”

6 120. With respect to Requirement 10, the PCI DSS explains that “[l]ogging
7 mechanisms and the ability to track user activities are critical in preventing, detecting, or
8 minimizing the impact of a data compromise. The presence of logs in all environments
9 allows thorough tracking, alerting, and analysis when something does go wrong.” It
10 further states, “[i]t is critical to have a process or system that links user access to system
11 components accessed. This system generates audit logs and provides the ability to trace
12 back suspicious activity to a specific user.” It also requires that merchants maintain
13 access to all audit trails because “[m]alicious users often attempt to alter audit logs to hide
14 their actions, and a record of access allows an organization to trace any inconsistencies or
15 potential tampering of the logs to an individual account.”

16 121. According to the Council, the essence of the overall Standard

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

(All emphasis in original.)

24 122. With respect to the “Assess” step, the Council instructs: “The primary goal
25 of assessment is to identify all technology and process vulnerabilities posing a risk to the
26 security of cardholder data that is transmitted, processed or stored by your business. ...
27 Determine how cardholder data flows from beginning to end of the transaction
28 process....” The Council tells merchants that “risk assessments can identify areas

1 containing data that need protection versus areas that are more open and do not need
2 access to sensitive data.”

3 123. The PCI DSS requires merchants to perform risk assessments. Risk
4 assessments are formal processes organizations use to identify threats and vulnerabilities
5 that could negatively impact the security of cardholder data. According to the Council,
6 during “a risk assessment, all vulnerabilities should be considered. ... Vulnerabilities may
7 be identified from vulnerability assessment reports, penetration-test reports and technical
8 security audits such as firewall rule reviews, secure code reviews and database
9 configuration reviews.” The Council provides a table of “examples of threats and
10 vulnerabilities,” which it emphasizes “is not an exhaustive list.” The table lists the first
11 example threat as “hackers, malicious individuals, cyber criminals,” identifies the first
12 potential vulnerability as “Lack of network security—e.g., properly configured firewalls,
13 lack of intrusion detection,” and warns that, if that vulnerability is exposed, it could lead
14 to “Network intrusion,” “System compromise,” “Compromise of sensitive data,” and
15 “Theft of CHD [cardholder data].”

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

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

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

8 127. The PCI DSS “strongly recommend[s]” “isolating (segmenting)[] the
9 cardholder data environment from the remainder of an entity’s network.” The PCI DSS
10 states that doing so may reduce the “risk to an organization.”

11 128. According to the Council, best practices in PCI security include: “Prior to
12 any modification to the [cardholder data] environment, all the systems and networks
13 affected by the change—including any new systems—should be identified. Questions that
14 should be considered include: ‘Do the changes introduce new connections between
15 systems in the CDE [cardholder data environment] and other systems that could bring
16 additional systems or networks into scope for PCI DSS?’ Other special considerations
17 should also be given to how the proposed change may affect technologies or any
18 underlying infrastructure that supports the security of the CDE, such as changes to
19 network-traffic routing rules, firewall rules, DNS configurations, or other security-related
20 functions.”

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

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

26 130. Healthcare patients and insurance plan members and beneficiaries are
27 generally aware of HIPAA as well as the fact that it and other laws and standards require
28

1 hospitals, clinics, and other health facilities to safeguard their PHI from unauthorized
2 disclosure.

3 131. The PCI Security Standards Council has stated that “[t]he public expects
4 that merchants ... will protect payment card data to thwart data theft and prevent
5 unauthorized use.”

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

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

14 134. At no time during the relevant time period did Banner disclose that its
15 information security was inadequate to reasonably safeguard the PII, PHI, and PCI to
16 which Banner was entrusted. Nor did Banner disclose that it had failed to follow the
17 [REDACTED] with respect to the protection of sensitive information,

18 [REDACTED]

19 [REDACTED]

20 [REDACTED] As Banner knew, such a disclosure would have been
21 material and contrary to the existing understanding of the patients, insureds, and other
22 customers of Banner, as well as Banner’s healthcare providers and employees.

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

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

28

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

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

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

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

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

1 141. Daniel Nutkis, the chief executive of the Health Information Trust Alliance,
2 a healthcare industry group that works with companies to improve data security, said in
3 2015 that “the industry has become, over the last three years, a much bigger target.”

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

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

14 144. On April 8, 2014, the Federal Bureau of Investigation (“FBI”) Cyber
15 Division issued a Private Industry Notification to healthcare providers, warning them that
16 their cybersecurity systems are inadequate. Per the notification, “the health care industry
17 is not technically prepared to combat against cyber criminals’ basic cyber intrusion
18 tactics, techniques and procedures (TTPs), much less against more advanced persistent
19 threats (APTs)” and “is not as resilient to cyber intrusions compared to the financial and
20 retail sectors, therefore the possibility of increased cyber intrusions is likely.” The
21 notification warned that cyberattacks against healthcare systems would increase due in
22 part to “mandatory transition from paper to electronic health records” and “a higher
23 financial payout for medical records in the black market.” The FBI also noted that it “has
24 observed malicious actors targeting healthcare related systems, perhaps for the purpose of
25 obtaining Protected Health Information (PHI) and/or Personally Identifiable Information
26 (PII).”

27 145. The FBI notification cited a report prepared by the SANS Institute warning
28 the healthcare industry that it was not adequately prepared to combat data breaches. The

1 report analyzed data collected between September 2012 and October 2013 and found the
2 results “alarming.” The report explained the data “not only confirmed how vulnerable the
3 industry had become, it also revealed how far behind industry-related cybersecurity
4 strategies and controls have fallen.”

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

10 147. In the fall 2014 national meeting of the NAIC, a Prudential Insurance Vice
11 President gave a presentation entitled “Cybersecurity & Insurance Companies.” The
12 presentation warned of the imminent threat to insurance companies’ data systems from
13 third-party threats. The presentation quoted U.S. Attorney General Eric Holder: “From
14 criminal syndicates, to terrorist organizations, to foreign intelligence groups, to
15 disgruntled employees and other malicious intruders, the range of entities that stand ready
16 to execute and exploit cyberattacks has never been greater.” The same presentation
17 contained a warning from the FBI director about the imminent risk of cyberattacks.

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

25 149. Robert Rost, Banner’s IT Operations Director of Defensive Services, gave a
26 conference presentation in March 2016 with others. The presentation explained that
27 electronic health record theft is a “[r]eal and growing threat to healthcare in 2016.” It
28

1 noted that “[e]xternal attacks are getting more sophisticated,” and may be perpetrated
2 through “[o]rganized crime.”

3 **IV. Banner Knew Its Information Security Was Inadequate.**

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

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

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

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

27 154. [REDACTED]
28 [REDACTED]
[REDACTED]

1 [REDACTED]
2 [REDACTED]
3 [REDACTED]
4 [REDACTED]
5 [REDACTED]

6 155. Another recommended form of network protection is application
7 whitelisting, which limits the applications that can be used on a server to only those
8 appearing on a preapproved list. Whitelisting essentially prevents malware applications
9 from being run on the system device, inhibiting and potentially stopping hackers from
10 being able to use their hacking tools. The NIST guidelines call for application
11 whitelisting in high-risk environments. It is the most important information security
12 control per the NSA's Information Assurance Directorate and the Australian Signals
13 Directorate and the second most important per the SANS Institute. Application
14 whitelisting is among the four controls that the Australian Signals Directorate says would
15 prevent 85 percent of cyber-intrusions. [REDACTED]

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

23 [REDACTED]
24 157. [REDACTED]
25 [REDACTED]
26 [REDACTED]
27 [REDACTED]
28 [REDACTED]

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

11 159. Up to and including June and July 2016, Banner’s network failed to comply
12 with all 12 PCI DSS requirements. [REDACTED]

13 [REDACTED]
14 [REDACTED]
15 160. [REDACTED]
16 [REDACTED] Such monitoring is standard in
17 the industry, and operating without it was unreasonable. The monitoring helps identify
18 potentially suspicious actions and access by unauthorized users within Banner’s network;
19 early detection of such activity can stop and minimize the likelihood of improper data
20 exfiltration.

21 161. Deloitte & Touche LLP (“Deloitte”), which is a leader in providing security-
22 specific advisory services to help companies assess, analyze, and improve their
23 information security. Deloitte is paid for its cybersecurity assessments by the companies
24 it assesses. On information and belief, Deloitte prepares the assessments and written
25 recommendations in a way designed to document its clients’ information security
26 deficiencies while seeking to avoid creating a record that could be used against the
27 companies in subsequent litigation in the event of a cyberattack.
28

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

162. [REDACTED]

[REDACTED]

163. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

164. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

165. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

166. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

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

167. [REDACTED]

[REDACTED]

168. [REDACTED]

[REDACTED]

1 169. [REDACTED]

2 [REDACTED]

3 [REDACTED]

4 [REDACTED]

5 [REDACTED]

6 170. [REDACTED]

7 [REDACTED]

8 [REDACTED]

9 [REDACTED] Banner

10 failed, however, to undertake those remedial measures up to and through the 2016 data

11 breach.

12 171. [REDACTED]

13 [REDACTED]

14 [REDACTED]

15 [REDACTED]

16 [REDACTED]

17 172. [REDACTED]

18 [REDACTED]

19 [REDACTED]

20 [REDACTED]

21 [REDACTED]

22 173. [REDACTED]

23 [REDACTED]

24 [REDACTED]

25 174. [REDACTED]

26 [REDACTED]

27 [REDACTED]

28 [REDACTED]

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

[Redacted text block]

175.

[Redacted text block]

[Redacted text block]

a.

[Redacted text block]

i.

[Redacted text block]

[Redacted text block]

[Redacted text block]

[Redacted text block]

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

[Redacted text block containing multiple lines of blacked-out content]

b. [Redacted text block containing multiple lines of blacked-out content]

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

[REDACTED]

[REDACTED]

i. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

ii. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

[Redacted text block]

c.

[Redacted text block]

i.

[Redacted text block]

ii.

[Redacted text block]

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

- [REDACTED]
- [REDACTED]
- d. [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- e. [REDACTED]
- i. [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- f. [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]

1 176. [REDACTED]

2 [REDACTED]

3 [REDACTED]

4 177. To address the issues identified in its 2014 assessment, [REDACTED]

5 [REDACTED]

6 178. [REDACTED]

7 [REDACTED]

8 [REDACTED]

9 [REDACTED]

10 [REDACTED] For example, in 2016, Banner still [REDACTED]

11 [REDACTED]

12 [REDACTED] failed to segment the network

13 and information on its network. [REDACTED]

14 [REDACTED]

15 Banner also did not establish an office of the Chief Information Security Officer until after

16 the data 2016 breach, with system level responsibility for information security at Banner.

17 179. [REDACTED]

18 [REDACTED]

19 [REDACTED]

20 [REDACTED]

21 180. [REDACTED]

22 [REDACTED]

23 [REDACTED]; thus, rather than exhibiting improvement in its information security, Banner was

24 moving in the wrong direction.

25 181. [REDACTED]

26 [REDACTED]

27 [REDACTED]

28 [REDACTED]

1 182. [REDACTED]

2 [REDACTED]

3 [REDACTED]

4 183. [REDACTED]

5 [REDACTED] Utilization of these “off the shelf” patches are

6 a fundamental aspect of network security; such patches often include security updates that

7 help protect the affected systems from unauthorized access and close known and

8 publicized security vulnerabilities. [REDACTED]

9 [REDACTED]

10 [REDACTED]

11 184. [REDACTED]

12 [REDACTED]

13 [REDACTED]

14 [REDACTED]

15 [REDACTED]

16 [REDACTED]

17 [REDACTED]

18 [REDACTED]

19 185. [REDACTED]

20 [REDACTED]

21 [REDACTED]

22 [REDACTED]

23 [REDACTED]

24 186. Prior to July 2016, Banner failed to remediate its security issues despite

25 several prior exposed failures on its part to protect PII and PHI. In 2014, Banner exposed

26 the Medicare identification and social security numbers of more than 50,000 people to

27 public view. Per a spokesperson, the error was caused by a problem with how Banner

28 processed mailing lists for its quarterly magazine. Using sensitive information like social

1 security numbers to organize mailing lists reflected a culture of reckless disregard of data
2 security. Also in 2014, the MyBanner portal experienced a data breach, in which patient
3 data was exposed to incorrect users. In response to the breach, senior management, IT
4 security, and the compliance group were not notified until about a month after the breach
5 was discovered.

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

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

13 188. [REDACTED]
14 [REDACTED]
15 [REDACTED]
16 [REDACTED]
17 [REDACTED]

18 189. [REDACTED]
19 [REDACTED]
20 [REDACTED]
21 [REDACTED]

22 190. [REDACTED]
23 [REDACTED]
24 [REDACTED]
25 [REDACTED]
26 [REDACTED]
27 [REDACTED]

28

1 191. The hackers first gained access to Banner's network on June 17, 2016, [REDACTED]

2 [REDACTED]

3 [REDACTED] The hackers authenticated to [REDACTED]

4 [REDACTED]

5 [REDACTED]

6 [REDACTED]

7 192. [REDACTED]

8 [REDACTED]

9 [REDACTED]

10 [REDACTED]

11 [REDACTED]

12 [REDACTED]

13 [REDACTED]

14 [REDACTED]

15 [REDACTED]

16 [REDACTED]

17 193. At the time of the hack, unencrypted PCI was sent to the exposed

18 [REDACTED] server, where it was encrypted and transmitted to the credit card company.

19 [REDACTED]

20 [REDACTED]

21 194. [REDACTED]

22 [REDACTED]

23 [REDACTED]

24 [REDACTED]

25 195. [REDACTED]

26 [REDACTED]

27 [REDACTED]

28 [REDACTED]

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

[Redacted]

[Redacted]

196. [Redacted]

[Redacted]

[Redacted]

[Redacted]

197. [Redacted]

[Redacted]

[Redacted]

[Redacted]

198. [Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

199. [Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

200. [Redacted]

[Redacted]

[Redacted]

201. [Redacted]

[Redacted]

[Redacted]

1 [REDACTED]
2 [REDACTED]
3 [REDACTED]
4 [REDACTED]
5 [REDACTED]

6 202. [REDACTED]
7 [REDACTED]

8 203. [REDACTED]
9 [REDACTED]
10 [REDACTED]
11 [REDACTED]

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

15 204. [REDACTED]
16 [REDACTED]
17 [REDACTED]
18 [REDACTED]
19 [REDACTED]
20 [REDACTED]

21 205. [REDACTED]
22 [REDACTED]
23 [REDACTED]
24 [REDACTED]

25 206. [REDACTED]
26 [REDACTED]
27 [REDACTED]

28

1 207. On June 21, 2016, the hackers logged into the [REDACTED] server using the
2 [REDACTED] account. [REDACTED]

3 [REDACTED]
4 [REDACTED]

5 On the same day, the hackers logged into the [REDACTED] server using the [REDACTED] user
6 account. [REDACTED]

7 [REDACTED]
8 [REDACTED]
9 [REDACTED]
10 [REDACTED]

11 208. [REDACTED]
12 [REDACTED]
13 [REDACTED]

14 209. [REDACTED]
15 [REDACTED]

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

19 211. [REDACTED]
20 [REDACTED]
21 [REDACTED]
22 [REDACTED]

23 212. Still on June 21, 2016, the hackers created files on the [REDACTED] server

24 [REDACTED]
25 [REDACTED]
26 [REDACTED]
27 [REDACTED]
28 [REDACTED]

1 [REDACTED]
2 [REDACTED] On information and belief, these databases contain PII
3 and PHI of Plaintiffs and Class Members.

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

9 214. [REDACTED]
10 [REDACTED]
11 [REDACTED]
12 [REDACTED]

13 215. [REDACTED]
14 [REDACTED]

15 216. On June 23, 2016, the hackers accessed the Banner database
16 [REDACTED]
17 [REDACTED]
18 [REDACTED]
19 [REDACTED]
20 [REDACTED]
21 [REDACTED]
22 [REDACTED]
23 [REDACTED]
24 [REDACTED]
25 [REDACTED]
26 [REDACTED]

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

1 218. [REDACTED]
2 [REDACTED]
3 [REDACTED]
4 [REDACTED]
5 [REDACTED]
6 [REDACTED]

7 219. [REDACTED]
8 [REDACTED]
9 [REDACTED]
10 [REDACTED]
11 [REDACTED]
12 [REDACTED]
13 [REDACTED]
14 [REDACTED]
15 [REDACTED]
16 [REDACTED]
17 [REDACTED]
18 [REDACTED]
19 [REDACTED]

20 220. [REDACTED]
21 [REDACTED]
22 [REDACTED]
23 [REDACTED]
24 [REDACTED]

25 221. In all, it took the hackers a total of approximately four days, from June 17 to
26 June 21, 2016, to access PII and PHI on Banner’s systems—a very short amount of time,
27 reflecting the ease with which the hackers were able to survey and move laterally within
28 Banner’s network. It took an additional two days, until June 23, 2016, to first access the

1 PCI of Banner food and beverage outlet customers. [REDACTED]

2 [REDACTED]

3 222. [REDACTED]

4 [REDACTED]

5 [REDACTED]

6 [REDACTED]

7 [REDACTED]

8 223. On June 29, 2016, Banner's IT team was asked to investigate system
9 slowness on various servers. [REDACTED]

10 [REDACTED]

11 [REDACTED]

12 [REDACTED]

13 224. [REDACTED]

14 [REDACTED]

15 [REDACTED]

16 225. On or around July 7, 2016, [REDACTED]

17 [REDACTED]

18 [REDACTED]

19 226. [REDACTED]

20 [REDACTED]

21 [REDACTED]

22 [REDACTED]

23 [REDACTED]

24 [REDACTED]

25 227. [REDACTED]

26 [REDACTED]

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

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

228. [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

[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]

[REDACTED]
229. [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

230. [REDACTED]
[REDACTED]
[REDACTED]

231. [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

1 [REDACTED]
2 [REDACTED]
3 232. Banner waited until August 3, 2016, to publicly announce that the data
4 breach had occurred, and said that all affected individuals would receive a breach
5 notification letter by September 9, 2016.

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

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

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

18 235. According to Banner, the data breach impacted a total of approximately 3.7
19 million people. That makes it the ninth largest healthcare data breach of all time, per the
20 OCR of HHS. According to a National Consumers League report, about one in three data
21 breach victims suffer identity fraud and that rate has increased in recent years.³

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

26 237. Banner acknowledged that the hackers accessed the servers where Banner
27 stored the PII and PHI of its patients and insurance plan members, including their names,

28 ³ 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).

1 birthdates, addresses, physicians' names, dates of service, claims information, clinical
2 information, health insurance information, and social security numbers.

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

7 239. The hackers compromised and accessed Banner server [REDACTED]

8 [REDACTED]
9 [REDACTED] The [REDACTED]
10 [REDACTED]
11 [REDACTED]
12 [REDACTED]
13 [REDACTED]
14 [REDACTED]
15 [REDACTED]
16 [REDACTED]

17 240. [REDACTED]

18 [REDACTED]
19 [REDACTED]
20 [REDACTED]
21 [REDACTED]
22 [REDACTED]

23 241. [REDACTED]

24 [REDACTED]
25 [REDACTED]
26 [REDACTED]
27 [REDACTED]

28

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

10 243. The social security numbers and other corroborating PII exposed through
11 the data breach create an imminent risk of identity fraud for Plaintiffs and the Class
12 Members. Criminals frequently use stolen social security numbers to create false bank
13 accounts, file fraudulent tax returns, file for unemployment benefits, or apply for a job
14 using a false identity. As the Social Security Administration has warned, identity thieves
15 can use an individual’s social security number and good credit score to apply for credit in
16 the name of the victim. This type of fraud can go undetected for years.

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

22 245. Generally, individuals cannot obtain a new social security number until *after*
23 evidence of ongoing problems caused by misuse already exists. Even then, the Social
24 Security Administration warns that “a new number probably won’t solve all [] problems .
25 . . and will not guarantee [] a fresh start.” For some victims of identity theft, “a new
26 number actually creates new problems.” In fact, according to Julie Ferguson, chair of the
27 Identity Theft Resource Center, the “credit bureaus and banks are able to link the new
28

1 number very quickly to the old number, so that old bad information is quickly inherited
2 into the new Social Security number.”

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

11 247. Unfortunately, though identity fraud is a common result from a data breach,
12 it is difficult to uncover. Individuals may not know that their social security numbers
13 have been used to file for unemployment benefits, for example, until law enforcement
14 becomes involved by notifying the individual’s employer of the suspected fraud (which,
15 in turn, may cause adverse consequences at work).

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

17 [REDACTED]
18 [REDACTED]
19 [REDACTED]
20 [REDACTED]
21 [REDACTED]
22 [REDACTED]
23 [REDACTED]

24 249. PCI is typically distributed quickly through private criminal networks or
25 sold on black market web forums on the so-called “Dark Web” to facilitate credit card
26 fraud. The customers whose PCI was compromised face the prospect of paying fees to
27 their banks for new debit and credit cards, paying fees to have the cards shipped faster so
28 that they do not have to wait weeks to make purchases on their accounts, and otherwise

1 dealing with the hassle, inconvenience, and distress of trying to resolve fraudulent
2 charges, obtain replacement payment cards, and correct information in their credit reports.
3 They also face the hassle and inconvenience of resetting autopayment functionality
4 following card replacement, as well as the prospect of late fees in the event a payment is
5 missed due to card cancellation on autopay accounts.

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

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

15 Examples include:

- 16 • complaints of a fraudulent bank account opened in their name, with the bank
17 “verif[ying] that her social security was used in the process”;
- 18 • “unauthorized applications” for credit at various retailers, including Kohl’s,
19 Sunglass Hut, and Guitar Center;
- 20 • receiving notice that a Citibank credit card “had been issued for \$11,000.00,” even
21 though “they did not apply for the card”;
- 22 • “receiv[ing] a collection call from PayPal for an account he never opened” and
23 being told by PayPal that “his social security number was associated with the
24 account”;
- 25 • “receiv[ing] a monitoring alert for 2 chase inquiries for applications she did not
26 authorize”;
- 27 • “receiving two credit cards in the mail that she did not apply for”;

- 1 • discovering applications of credit where a creditor “confirmed use of his
- 2 information”;
- 3 • “receiv[ing] a letter from Capital One advising an application for a credit card was
- 4 received that she did not authorize”;
- 5 • “receiv[ing] a credit card from Compass bank that she did not apply for” with
- 6 verification that “an account was established without her consent”;
- 7 • receiving an alert for a new account with Discover and two letters from Chase
- 8 concerning applications for an American Visa Signature card, with verification that
- 9 the breach victim’s “SSN was used for applications and account”;
- 10 • receiving “a letter that they are needing a cashiers check for a condo he was buying
- 11 only [he] is not buying a condo”;
- 12 • and discovering that someone had “filed a fraudulent tax return with the member’s
- 13 information”;
- 14 • Plaintiff Halpin’s experiences of identity fraud including two accounts that were
- 15 fraudulently opened in her name, and an unauthorized person filing taxes using her
- 16 social security number; and
- 17 • Plaintiff Maryniak’s unauthorized account use and attempted use.

18 252. Individuals whose PHI is compromised in data breaches are also particularly
19 susceptible to tax return fraud. Using stolen PII, cyber criminals file tax returns in the
20 name and social security number of the victim, seeking refunds under the guise of the
21 victim taxpayer. In 2013, according to the Government Accountability Office, the IRS
22 paid an estimated \$5.2 billion in tax refunds obtained from identity theft; it prevented an
23 additional \$24.2 billion in fraudulent transfers that year. It is estimated that in 2016 there
24 will be \$21 billion in losses due to fraudulent tax refunds, and data breaches are large
25 factor contributing to this form of identity theft. The U.S. Treasury Inspector General for
26 Tax Administration has recognized that “[t]he increasing number of data breaches in the
27 private and public sectors means more personal information than ever before is available
28 to unscrupulous individuals.” Fraudulent tax returns are typically discovered only when

1 an individual's authentic tax return is rejected. It can take months or years, as well as
2 significant expense to the victim, to correct the fraud with the IRS.

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

10 254. Medical records obtained through a data breach can thus be worth
11 hundreds of dollars per individual. Bob Gregg, chief executive of ID Experts,
12 explained that "detailed medical records with unique patient identifying numbers
13 can fetch up to \$100 per record," compared with \$1 to \$3 for a record containing a
14 name, address, and social security number. Another security expert said that, at a
15 black market auction, a patient medical record sold for \$251, compared to credit
16 card records selling for thirty-three cents. According to a PricewaterhouseCoopers
17 report, a "complete identity-theft kit containing comprehensive health insurance
18 credentials can be worth hundreds of dollars or even \$1,000 each on the black
19 market." Marc Probst, chief information officer of Intermountain Healthcare in
20 Salt Lake City, said his hospital system fends off thousands of attempts to penetrate
21 its network each week. "The only reason to buy that data is so they can
22 fraudulently bill," Probst said.

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

25 256. Medical identity theft victims spend, on average, \$13,500 to resolve
26 problems stemming from medical identity theft, which for many included out-of-pocket
27 costs for healthcare they did not receive in order to regain coverage. Victims of medical
28 identity theft may also lose their healthcare coverage or experience increased premiums.

1 And, studies have shown that a significant percent of medical identity victims are never
2 able to resolve their identity theft.

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

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

20 259. According to a 2015 Ponemon Institute study, only ten percent of
21 respondents report “achieving a completely satisfactory conclusion” of the medical
22 identity theft incident. Those who have resolved the crime “spent, on average, more than
23 200 hours on such activities as working with their insurer or healthcare provider to make
24 sure their personal medical credentials are secured . . . and verifying their personal health
25 information, medical invoices and claims and electronic health records are accurate.”
26 Most victims of medical identity theft do not learn about the theft until more than three
27 months after it has occurred. Due to time and energy spent monitoring one’s information
28 and correcting false information, medical fraud also takes an emotional toll on its victims.

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

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

12 262. Kroll's offered services were to monitor only one of the three major credit
13 reporting bureaus, TransUnion, leaving unattended sources from the other credit reporting
14 bureaus from which identity theft can be detected. Individuals had to sign up for the Kroll
15 services online, but many reported that when they visited the website, their security
16 software identified the website as unsecure. As a result, many were "apprehensive" about
17 signing up because they wanted to avoid "any chance of additional exposure by using an
18 unsecure site." Others, including elderly and lower income individuals, did not have
19 computer access and therefore did not sign up for Kroll's services. Still others share an
20 email address with their spouses, and Kroll did not permit them to sign up for two
21 separate credit monitoring accounts.

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

28

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

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

25 266. Finally, Banner has not offered to reimburse any costs associated with
26 pursuing preventive measures—even those recommended by the FTC. The FTC
27 recommends taking multiple steps depending upon the circumstances, including placing a
28 fraud alert, requesting a credit freeze, ordering credit reports, creating an identity theft

1 report, and filing a police report. To guard against medical identity theft, individuals
2 should routinely obtain the most recent copies of their medical records and inspect them
3 for discrepancies. In addition, credit bureaus charge approximately \$30 to freeze credit
4 reports, which can be avoided only by filing a police report. Banner is aware of these
5 costs, yet continues not to assist with them.

6 **CLASS ACTION ALLEGATIONS**

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

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

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

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

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

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

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

28

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

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

- 13 a. Banner was obligated to safeguard Plaintiffs' and the Class Members' PII,
14 PHI, and PCI;
- 15 b. Banner breached its obligation to safeguard Plaintiffs' and the Class
16 Members' PII, PHI, and PCI;
- 17 c. Banner failed to implement reasonable, industry-standard safeguards for
18 Plaintiffs' and the Class Members' PII, PHI, and PCI;
- 19 d. Banner failed to disclose its inability, to adequately safeguard Plaintiffs' and
20 the Class Members' PII, PHI, and PCI;
- 21 e. Banner's inadequate information security practices violated federal and state
22 law;
- 23 f. Banner's failure to safeguard Plaintiffs' and the Class Members' PII, PHI,
24 and PCI led to a data breach in 2016 during which the security of Plaintiffs'
25 and the Class Members' PII, PHI, and PCI was compromised;
- 26 g. Banner's inadequate information security practices have harmed Plaintiffs
27 and the Class Members and have put them at imminent risk of future harm;

- 1 h. Banner failed to take reasonable steps to mitigate the effects of the data
2 breach, including by failing to notify Plaintiffs and Class Members about the
3 data breach as soon as practicable after its discovery;
- 4 i. Banner should return the money paid by Plaintiffs and Class Members to
5 protect their PII, PHI, or PCI;
- 6 j. Plaintiffs and Class Members are entitled to damages, restitution, or some
7 other form of remuneration as a result of Banner's wrongful conduct; and
- 8 k. Injunctive or other equitable relief is appropriate to redress Banner's
9 wrongful conduct and, if so, what form it should take.

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

14 273. **Adequacy of Representation**: Plaintiffs are adequate representatives of the
15 proposed classes because neither their nor their counsel's interests conflict with the
16 interests of the members of the Classes they seek to represent. Plaintiffs have retained
17 counsel competent and experienced in complex class action litigation and will prosecute
18 this action vigorously on Class Members' behalf.

19 274. **Superiority**: A class action is superior to other available means for the fair
20 and efficient adjudication of this dispute. The injury suffered by each Class Member,
21 while meaningful on an individual basis, is not of such magnitude as to make the
22 prosecution of individual actions against Banner economically feasible. Even if Class
23 Members themselves could afford such individualized litigation, the court system could
24 not. In addition to the burden and expense of managing many actions arising from the
25 data breach, individualized litigation presents a potential for inconsistent or contradictory
26 judgments. Individualized litigation increases the delay and expense to all parties and the
27 court system presented by the legal and factual issues of the case. By contrast, a class
28

1 action presents far fewer management difficulties and provides the benefits of single
2 adjudication, economy of scale, and comprehensive supervision by a single court.

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

- 4 a. The prosecution of separate actions by the individual members of the
5 proposed class would create a risk of inconsistent adjudications, which
6 could establish incompatible standards of conduct for Banner;
- 7 b. The prosecution of individual actions could result in adjudications, which as
8 a practical matter, would be dispositive of the interests of non-party class
9 members or which would substantially impair their ability to protect their
10 interests; and
- 11 c. Banner has acted or refused to act on grounds generally applicable to the
12 proposed Classes, thereby making appropriate final and injunctive relief
13 with respect to the members of the proposed classes as a whole.

14 **FIRST CAUSE OF ACTION**

15 **Negligence**

16 **(All Plaintiffs on behalf of the proposed Classes)**

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

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

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

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

26 280. Banner was required to secure and safeguard the PII, PHI, and PCI of
27 Plaintiffs and Class Members, to prevent disclosure of the information, and to guard the
28 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

1 reasonably expeditious period of time so that it could respond, remedy, and promptly
2 notify affected individuals in the event of a security breach. Banner was further required
3 to maintain PII, PHI, and PCI as long as necessary and required by law.

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

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

- 9 a. 45 C.F.R. § 164.306(a)(1) for failing to ensure the confidentiality and
10 integrity of electronic PII and PHI that Banner created, received, and
11 maintained from Plaintiffs and Class Members.
- 12 b. 45 C.F.R. § 164.306(a)(2) for failing to protect against reasonably
13 anticipated threats or hazards to the security or integrity of the electronic PII
14 and PHI of Plaintiffs and Class Members;
- 15 c. 45 C.F.R. § 164.306(a)(3) for failing to protect against reasonably
16 anticipated uses or disclosures of electronic PHI not permitted under the
17 privacy rules regarding individually identifiable health information;
- 18 d. 45 C.F.R. § 164.306(a)(4) for failing to ensure compliance with the HIPAA
19 security standard rules; and
- 20 e. 45 C.F.R. § 164.308(a)(1)(i) for failing to implement policies and
21 procedures to prevent, detect, contain and correct security violations.

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

27 284. Plaintiffs and Class Members have suffered harm as a result of Banner's
28 breach of duty. The PII, PHI, and PCI of Plaintiffs and Class Members was exposed,

1 subjecting each Class member to identity theft, credit and bank fraud, social security
2 fraud, tax fraud, medical identity fraud and other varieties of identity fraud.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

26 305. As set forth above, all Plaintiffs and Class Members who were employed by
27 Banner entered into contracts that include, either by express provision or attachment, or
28 incorporation by reference, Banner's then-current privacy policies pertaining to

1 employees' and health care providers' personally identifiable information, including but
2 not limited to the Employee Handbook and the Banner Workforce Confidentiality Policy.

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

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

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

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

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

27 310. Plaintiffs reallege the paragraphs above as if fully set forth herein.
28

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

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

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

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

14 315. As set forth above, Banner promised to protect Plaintiffs' and Class
15 Members' PII and PHI. Even if Banner is held not to have breached any express promise
16 in these contracts, Banner breached the covenant of good faith and fair dealing by failing
17 to take adequate measures to protect the confidentiality of Plaintiffs' and Class Members'
18 PII and PHI, resulting in the June and July 2016 data breach. Banner unreasonably
19 interfered with the contract benefits owed to Plaintiff and Class Members by: compiling
20 and storing Plaintiff and Class Members' data with unreasonable and inadequate
21 cybersecurity protections and by permitting unrestricted access to the PII and PHI
22 entrusted to it.

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

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

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

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

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

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

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

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

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

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

28 324. The contracts, between Banner, on one hand, and Plaintiffs and Class
Members, on the other hand, were an undertaking for consideration, which bestowed a

1 duty upon Banner to perform its contractual obligations competently and with reasonable
2 care.

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

9 326. Banner failed to perform its obligations competently and with reasonable
10 care because it failed to take reasonable and adequate measures to protect the
11 confidentiality of Plaintiffs' and Class Members' PII and PHI, resulting in the June and
12 July 2016 data breach. Banner compiled, stored, and used Plaintiffs' and Class Members'
13 data using unreasonable and inadequate cybersecurity protections and permitted
14 unrestricted access to the PII and PHI entrusted to it.

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

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

1 disclose and concealed material facts and information as alleged herein, despite its duty to
2 do so.

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

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

11 346. Plaintiffs and the Class Members seek all available relief under A.R.S. §
12 4421, *et. seq.*, including, but not limited to, compensatory damages, punitive damages,
13 injunctive relief, and attorneys' fees and costs.

14 **PRAYER FOR RELIEF**

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

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

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

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

23 D. An award of punitive damages;

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

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

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

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

3 **DEMAND FOR JURY TRIAL**

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

6 RESPECTFULLY SUBMITTED and dated this 3rd day of March, 2017.

7 **GALLAGHER & KENNEDY, P.A.**

8 By: /s/ Paul L. Stoller

9 Paul L. Stoller
10 Lincoln Combs
11 2575 E. Camelback Road, Suite 1100
12 Phoenix, Arizona 85016-9225

13 Andrew S. Friedman
14 William F. King
15 **BONNETT FAIRBOURN FRIEDMAN &
16 BALINT, P.C.**
17 2325 E. Camelback Road, Suite 300
18 Phoenix, Arizona 85016

19 *Interim Co-Lead Class Counsel*

20 Eric H. Gibbs (pro hac vice)
21 David Stein (pro hac vice)
22 Amanda M. Karl (pro hac vice)
23 **GIRARD GIBBS LLP**
24 505 14th Street, Suite 1110
25 Oakland, California 94612
26 ehg@classlawgroup.com
27 ds@classlawgroup.com
28 amk@classlawgroup.com

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

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@hbsslw.com
leonard@hbsslw.com
michellak@hbsslw.com

Executive Committee

CERTIFICATE OF SERVICE

I hereby certify that on, March 3, 2017, 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

5880011