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

As local counsel on behalf of:

Benjamin F. Johns
Andrew W. Ferich
CHIMICLES & TIKELLIS LLP
One Haverford Centre
361 Lancaster Avenue
Haverford, PA 19041
(610) 642-8500
bfj@chimicles.com
awf@chimicles.com

Counsel for Plaintiff and the Putative Class (*pro hac vice* application to be filed)

UNITED STATES DISTRICT COURT
DISTRICT OF ARIZONA

Kendra Clark, individually and on behalf of all others similarly situated,

Plaintiff,

v.

Banner Health,

Defendant.

Case No.

CLASS ACTION COMPLAINT
DEMAND FOR JURY TRIAL

Plaintiff Kendra Clark ("Plaintiff"), individually and on behalf of all others similarly situated, based on personal knowledge as to her own acts and experiences and on investigation of counsel as to all other matters, alleges as follows:

NATURE OF THE ACTION

1. Plaintiff brings this action, individually and on behalf of all others similarly situated whose personal and non-public information, including names, addresses, birthdates, telephone numbers, Social Security numbers, credit card information, medical information (physician names, dates of service, clinical information, insurance information, *etc*.), and physician or provider credentials (DEA registration numbers, National Provider Identifiers, *etc.*) was compromised in a massive breach of Defendant Banner Health's ("Banner Health" or "Banner") computer servers.

2. On August 3, 2016, Banner Health publicly announced that its computer systems suffered a massive cyberattack that may affect 3.7 million people, making it the largest data breach of 2016.

3. Unlike some data breaches where only credit card information is stolen, Banner Health's data breach also exposed extremely sensitive information of 3.7 million patients, health plan members (and their beneficiaries), food and beverage customers, and physicians and healthcare providers. Information such as birth dates, names, addresses, Social Security numbers, medical data, and personal identifying information are especially valuable to cyber criminals because they cannot be readily changed or canceled (unlike credit cards) and can be used to perpetrate other frauds, including the creation of false records for identity theft.

4. On August 3, 2016, Banner Health issued a statement[1] identifying that it

[1] A full copy of Banner Health's statement concerning the data breach is located at https://www.bannerhealth.com/news/2016/08/banner-health-identifies-cyber-attack (last visited Aug. 8, 2016).

first learned of a massive cyberattack on July 7, 2016, although the attack supposedly began on June 17, 2016.

5. The attack was first reported to have started with fraudsters targeting data from credit cards, including card holder names, card numbers, expiration dates, and security codes. This attack was initially reported to have begun on June 23, 2016.

6. Then on July 13—six days after Banner learned of the June 23 attack—Banner subsequently learned that attackers "may have gained unauthorized access to patient information, health plan member and beneficiary information, as well as information about physician and healthcare providers" beginning on June 17, 2016.[2]

7. According to Banner's August 3 statement, "[t]he patient and health plan information may have included names, birthdates, addresses, physicians' names, dates of service, claims information, and possibly health insurance information and social security numbers."[3]

8. As part of its August 3, 2016 statement, Banner Health also announced it is mailing letters to the 3.7 million potentially affected customers.

9. To date, Banner Health – without providing any details – has merely identified that it has "launched an investigation, hired a leading forensics firm, took steps to block the cyber attackers and contacted law enforcement" and that it "is working to enhance the security of its systems in order to help prevent this from happening in the future."[4] The letter Banner is sending to the 3.7 million affected individuals and entities provides no information beyond what Banner has already released in its August 3 statement.

10. Other than confirming that Banner Health's servers have been

[2] https://www.bannerhealth.com/news/2016/08/banner-health-identifies-cyber-attack (last visited Aug. 8, 2016).
[3] *Id.*
[4] *Id.*

compromised, Banner Health has failed to provide any in-depth or detailed information as to the actual extent of this compromise, such as the security vulnerabilities that led to the breach, what (if any) measures have been implemented to prevent subsequent data breaches and their effectiveness, and the full extent of compromised information.

11. This data breach is the direct result of Banner Health's failure to implement adequate cybersecurity measures commensurate with the duties it undertook by storing large amounts of customer information on its computer servers. Indeed, Banner Health knew that it was storing sensitive information on its servers that is valuable and vulnerable to cyber attackers. The data collected and stored by healthcare providers like Banner Health is among the most highly sensitive personally identifiable information, and these companies thus bear the crucial responsibility to protect this data from compromise and theft.

12. In short, Banner Health breached its duty to protect and safeguard Class Members' personal, health, and financial information and to take reasonable steps to contain the damage caused where any such information was compromised. Through no fault of their own, Class Members have suffered financial and emotional injury and must now attempt to safeguard themselves and their families from unknown but certainly impending future crimes. For the reasons set forth below, Plaintiff and Class Members request damages to compensate them for current and future losses, as well as injunctive relief to provide safeguards against another failure of Banner Health's cybersecurity systems.

13. In addition, and while Plaintiff recognizes that Banner is offering a free one-year membership in monitoring services to those affected by this data breach, Plaintiff and Class Members allege that this provision is inadequate to ensure future security of personal and sensitive information, particularly where it includes that of minor children and the elderly. Plaintiff and Class Members therefore seek credit

monitoring services (and other appropriate relief) uniquely tailored to protect not only the interests of able-bodied adults but also the more vulnerable victims of this data breach, namely minors, as well as retention of a service to assist the elderly and infirm victims of this breach to monitor their credit and proactively guard against future identity theft and fraud.

PARTIES

14. Plaintiff Kendra Clark is a resident of Scottsdale, Arizona. Plaintiff Clark is a physician assistant and medical services provider within the Banner Health system. On or about August 8, 2016, Plaintiff received a letter from Banner informing Plaintiff that she has been victimized by a cyberattack that may have affected the security of her personal and protected information, including her "name, address, date of birth, DEA (Drug Enforcement Agency) number, TIN (Tax Identification Number), NPI (National Provider Identifier), or Social Security number." A redacted copy of this letter is attached hereto as **Exhibit "A."** Like Banner's statement of August 3, 2016 regarding the data breach, the letter sent to Plaintiff contains hardly any detail about the cyberattack, and does not specify exactly which of Plaintiff's information was stolen. Plaintiff's information remains at high risk for fraud, including identity theft. As a result of Banner's conduct alleged herein, Plaintiff has been harmed and will continue to be exposed to the risk that she will be victimized by identity theft or some other form of fraud.

15. Defendant Banner Health is a non-profit corporation that incorporated in the state of Arizona and has a principal place of business located at 2901 N. Central Ave., Suite 160, Phoenix, Arizona, 85012. Banner Health is also incorporated under the laws of the state of Alaska (entity #76903F). For the fiscal year ended December 31, 2015, Banner Health reported that it (and its subsidiaries) had $6.971B in total revenues, along with $6.843B in operating expenses.

JURISDICTION AND VENUE

16. This Court has subject matter jurisdiction pursuant to 28 U.S.C. § 1332, as amended by the Class Action Fairness Act of 2005, because the matter in controversy exceeds $5 million, exclusive of interest and costs, and is a class action in which some members of the Class are citizens of states different than Defendant. *See* 28 U.S.C. § 1332(d)(2)(A). This Court also has supplemental jurisdiction over the state law claims pursuant to 28 U.S.C. § 1367.

17. This Court has personal jurisdiction over Defendant. Defendant has sufficient minimum contacts with the state of Arizona and intentionally avails itself of the consumers and markets within the state through the promotion, marketing, and sale of its health, medical, and other services.

18. Venue properly lies in this district pursuant to 28 U.S.C. § 1391(a)(2) because Defendant conducts substantial business in this district, is headquartered in this district, and is deemed to be a citizen of this district. A substantial part of the events and/or omissions giving rise to the claims occurred, in part, within this district.

FACTUAL ALLEGATIONS

19. Banner Health is a health system operating in Alaska, Arizona, California, Colorado, Nebraska, Nevada, and Wyoming. It operates 29 hospitals, including three academic medical centers and other related health entities and services, with more than 47,000 employees. Banner identifies itself as the largest private employer in Arizona and the third largest employer in the Northern Colorado front range area. A map showing Banner's locations of operations is depicted below:

20. In the wake of the massive data breach of Banner Health's computer servers from June to July 2016, Banner has urged that "Banner Health is committed to maintaining the privacy and security of personal information we maintain on behalf of our patients, health plan members, employees, providers and all of their families."[5] But Banner Health could not seriously have been "committed" to these cyber security goals in light of the circumstances surrounding the data breach which affected approximately 3.7 million customers.

[5] *Id.*

21. On August 3, 2016, Banner first acknowledged in a public statement (the "Statement") that beginning on June 23, 2016, hackers gained unauthorized access to Banner Health's computer servers.

22. According to the Statement, Banner's initial discovery was that the attackers targeted payment card data, including cardholder names, card numbers, expiration dates, and security codes, for payment cards used at Banner facilities across the country.

23. Banner has identified that food and beverage outlets affected during the two-week period between June 23 and July 7, 2016 are located in Alaska, Arizona, Colorado, and Wyoming.[6]

24. According to Banner Health, this portion of the cyberattack continued until July 7, 2016 – the date on which Banner Health supposedly first learned of the data breach. Banner Health merely stated that it "worked quickly to block the attackers"[7] without providing any more information as to what steps it took to stop the attack and to ensure that the attack would not continue or resume, or that its servers would not be subjected to another attack of this type.

25. Also in its Statement, Banner identified that on July 13 it subsequently learned that the attack ran deeper than the credit card information attack that began on June 23. Banner announced that beginning a week earlier on June 17, 2016, attackers "may have" gained unauthorized access to patient information, health plan member and beneficiary information, and information about physicians and healthcare providers.

26. To date, Banner has not confirmed whether the attackers who breached Banner's servers beginning June 17 *actually* succeeded in obtaining this information. As

[6] http://bannersupports.com/customers/affected-locations/ (last visited Aug. 8, 2016).
[7] https://www.bannerhealth.com/news/2016/08/banner-health-identifies-cyber-attack (last visited Aug. 8, 2016).

one news report plainly identified, "[i]n other words the breaches had taken place three weeks (and in the case of the Banner Health servers, nearly four weeks) before the company realised any intrusion had occurred."[8]

27. Although Banner has not been able to identify with any sense of certainty the extent of the attack or the exact information and data obtained by the attackers, Banner Health spokesman Bill Byron identified that the attack is "extensive throughout the [Banner Health] network."[9]

28. Banner did not make it a top priority to report this breach to its customers immediately. It was only on August 3, 2016 – almost an entire month after Banner learned of this breach – that Banner Health decided it would issue the Statement acknowledging the cyberattack.

29. The Statement is underwhelming. The lack of details contained in the Statement signals that Banner is either withholding information from the public (most importantly its customers) or that, despite the passage of nearly two months since the attack began, Banner has been unable to determine critical details concerning the breach, including the extent of the breach and the volume of compromised information.

30. Boiled down, Banner's Statement only really goes so far as to provide the following details:

- Banner learned of the attack on July 7, 2016 and it began starting on June 17, 2016;
- the data breach affects approximately 3.7 million customers;

[8] Warwick Ashford, Banner Health cyber breach underlines need for faster intrusion detection, available at http://www.computerweekly.com/news/450301995/Banner-Health-cyber-breach-underlines-need-for-faster-intrusion-detection (last visited Aug. 8, 2016).

[9] Pat Ferrier, Banner Health cyberattack breaches health, SSN, credit card data, located at http://www.coloradoan.com/story/money/business/2016/08/03/banner-health-cyberattack-breaches-health-ssn-credit-card-data/88036664/ (last visited Aug. 8, 2016).

- the attack targeted payment card data and "may have" targeted sensitive personal, medical and financial information;
- Banner took (unidentified) steps to block the attackers and to make sure the attack does not continue;
- Banner is investigating the attack; and
- Banner is offering free-credit monitoring for one year and will issue letters to the approximately 3.7 million affected customers.[10]

31. The letter that has been sent or that is being sent by Banner to affected customers is equally devoid of information and details regarding the breach. The letter identifies: the barebones details of the timeline of the data breach; that customer information (names, birthdates, addresses, clinical information, Social Security numbers, insurance information, *etc.*) "may have" been obtained by attackers; that affected customers are being offered one year of free credit-monitoring services from Kroll; and – without providing any information regarding how the breach actually occurred or the exact measures that Banner will take going forward – that Banner is "further enhancing the security of [its] systems to help prevent something like this from happening again." *See, e.g.*, Exhibit A.

32. The lack of information provided by Banner to date regarding this cyberattack is alarming. For example, Banner has not stated with certainty whether the attackers gained access to private and sensitive customer information – only that they "may have" done so.[11] Furthermore, while the security measures (or lack thereof) taken by Banner Health to prevent this attack were clearly inadequate and precipitated this data

[10] https://www.bannerhealth.com/news/2016/08/banner-health-identifies-cyber-attack (last visited Aug. 8, 2016).

[11] *See* http://bannersupports.com/ (last visited Aug. 8, 2016).

breach, its actions and the precautions or measures it is taking subsequent to the cyberattack have been inexplicably unclear and superficial.

33. Banner has even had the audacity to implore customers to resume using payment cards at Banner facilities so that it can continue to make money, stating that customers can do so "with confidence."[12] But customers like Plaintiff and Class Members are anything but confident that their information is secure and will not be used to perpetrate future crimes – including identity theft – in light of Banner's nonchalant response to this incident.

34. Banner's response to this incident is particularly egregious given the number and magnitude of data breaches experienced across the United States recently.

35. Over the past couple of years, large data breaches and cyberattacks have become somewhat commonplace, as evidenced by the widely publicized incidents at Target, Home Depot, Anthem, and many others. With 3.7 million potentially affected customers, the Banner Health breach is the largest of 2016 and would be the eighth largest attack according to HHS' Office for Civil Rights. As a result of the frequency of these types of cyber security breaches, companies that store and maintain confidential and highly sensitive information must develop, implement, and maintain up-to-date data security and retention policies that reduce the risk of cyberattack and unauthorized release of this information. But many companies do not take these precautions or the measures taken fall short of being adequate.

36. Following the Banner breach, one cyber security expert noted the tendency of large companies to fall short of their obligations to consumers with respect to privacy and data protection. "Most of the time these healthcare organizations have no systems in place to alert them when lots of data is being sucked out using some privileged account,"

[12] *Id.*

said Mansur Hasib, program chair of cybersecurity technology at the University of Maryland University College graduate school, and author of the book entitled "Cybersecurity Leadership."[13]

37. According to another cyber security expert, Chris Ensey, chief operating officer of Dunbar Security Solutions in Hunt Valley, Maryland, following a breach of this magnitude a company's IT personnel would need to restart the entire network from scratch and reset all the components of the network to the state they were in when they arrived from the factory in order to be certain the breach has been fixed. He also identified that there is a chance hackers created a "back door" in the initial breach that may not be caught. Ensey stated "That would make me, if I were in the shoes of the folks there, really struggle with being able to sleep at night for a while, until they had the opportunity to do a complete overhaul . . . ."[14]

38. But Banner merely identifies that it is still investigating to find out exactly what happened, and spokesman Byron said he cannot say when the investigation will be concluded, stating "I don't know that there is a timeline . . . The goal is to complete the investigation."[15]

39. Victims of Banner's data breach have suffered, or are at imminent risk of further suffering, identity theft and medical identity theft because "[w]hen someone has your clinical information, your bank account information, and your Social Security number, they can commit fraud that lasts a long time. Th[is] kind of identity theft . . . is

[13] Bill Siwicki, Banner Health nailed by huge cyberattack that compromised personal data of 3.7 million people, available at http://www.healthcareitnews.com/news/banner-health-nailed-huge-cyberattack-compromised-personal-data-37-million-people (last visited Aug. 8, 2016).

[14] Nate A. Miller, Experts: Banner Health cyberattack is part of trend among hackers to target health care providers, available at http://www.greeleytribune.com/news/23259877-113/experts-banner-health-cyberattack-is-part-of-trend# (last visited Aug. 8, 2016).

[15] *Id*.

qualitatively and quantitatively different than what is typically possible when you lose your credit card . . . ."[16]

40. Victims of Banner's data breach face a number of other frustrating and challenging hurdles. For example, victims of a data breach of this type face imminent risk of health insurance discrimination. Individuals risk denial of coverage, improper "redlining," and denial or difficulty obtaining disability or employment benefits because information was improperly disclosed to a provider.

41. Victims of healthcare data breaches are also particularly susceptible to tax return fraud. It is estimated that in 2016 there will be $21 billion in losses due to fraudulent tax refunds, and data breaches are large factor contributing to this reality. The U.S. Treasury Inspector General for Tax Administration has recognized that "[t]he increasing number of data breaches in the private and public sectors means more personal information than ever before is available to unscrupulous individuals."[17]

42. The information compromised in this data breach is significantly more valuable to a cyber attacker than, say, credit card information obtained in a large retailer data breach. Victims of retailer breaches could avoid much of the potential for future harm by cancelling credit or debit cards and obtaining replacements. The information compromised in the Banner breach is difficult, if not impossible, to change—social security numbers, names, dates of birth, employment information, income data, medical or clinical information, *etc.*

[16] Premera Hack: What Criminals Can Do With Your Healthcare Data, Christian Science Monitor, Jaikumar Vijayan, Mar. 20, 2015, available at http://www.csmonitor.com/World/Passcode/2015/0320/Premera-hack-What-criminalscan-do-with-your-healthcare-data (last visited Aug. 7, 2016).

[17] Susan Tompor, Tax refund losses could reach $21B this year, available at http://www.freep.com/story/money/personal-finance/susan-tompor/2016/04/18/tax-refund-losses-could-reach-21b-year/83023206/ (last visited Aug. 9, 2016).

43. Despite having knowledge of the recent wave of high-profile data breaches and the need for heightened security measures, Banner Health failed to develop, implement, and maintain data security and retention policies that reflect industry standards. Had Banner done so, it would have both detected the breach earlier and helped reduce the severity of the breach, or potentially would have prevented the breach entirely.

44. This catastrophic and complete failure by Banner resulted in increased exposure to data breaches, and caused the release of consumers' personal and medical data. The release of this information will likely lead to identity theft and fraud-related issues for the months and years to come.

45. Furthermore, there is no indication by its words or deeds that Banner is approaching and responding to this security catastrophe with an utter and necessary sense of urgency.

46. As of the date of this Complaint, there is no indication as to whether Banner Health has implemented recommended security improvements, leaving Plaintiff and Class Members' data vulnerable to future data breaches.

CLASS ALLEGATIONS

47. Plaintiff brings this action on her own behalf, and on behalf of the following Class pursuant to FED. R. CIV. P. 23(b)(2) and (3):

> All former or present Banner Health patients, health plan members or health plan beneficiaries, food and beverage customers, or medical and healthcare providers who had their personal, medical, financial, or other sensitive information compromised as a result of the data breach of Banner Health's computer servers that began on June 17, 2016.

48. Excluded from the Class are Defendant, its affiliates, officers, directors, assigns, successors, and the Judge(s) assigned to this case. Plaintiffs reserve the right to modify, change, or expand the definitions of the Class based on discovery and further investigation.

49. **Numerosity**: Members of the Class are so numerous that their individual joinder is impracticable, as the proposed Class appears to include millions of members who are geographically dispersed. While the precise number of Class members has not yet been determined, Banner Health has admitted that the medical, financial, and/or personal identification records of approximately 3.7 million patients, health plan members (and their beneficiaries), food and beverage customers, and physicians and healthcare providers were likely compromised in the data breach.

50. **Typicality**: Plaintiff's claims are typical of the claims of the Class. Plaintiff and all members of the Class were injured through Banner's uniform misconduct. The same event and conduct that gave rise to Plaintiff's claims are identical to those that give rise to the claims of every other Class member because Plaintiff and each member of the Class had their data compromised in the same way by the same conduct by Banner.

51. **Adequacy**: Plaintiff is an adequate representative of the Class because her interests do not conflict with the interests of the Class that they seek to represent; Plaintiff has retained counsel competent and highly experienced in class-action litigation; and Plaintiff and her counsel intend to prosecute this action vigorously. The interests of the Class will be fairly and adequately protected by Plaintiff and her counsel.

52. **Superiority**: A class action is superior to other available means of fair and efficient adjudication of the claims of Plaintiff and the Class. The injury suffered by each individual Class member is relatively small in comparison to the burden and expense of individual prosecution of complex and expensive litigation. It would be very difficult if not impossible for members of the Class individually to effectively redress Defendant's wrongdoing. Even if Class members could afford such individual litigation, the court system could not. Individualized litigation presents a potential for inconsistent or contradictory judgments. Individualized litigation increases the delay and expense to

all parties, and to the court system, presented by the complex legal and factual issues of the case. By contrast, the class-action device presents far fewer management difficulties and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court.

53. **Existence and Predominance of Common Questions of Fact and Law**: Common questions of law and fact exist as to all members of the Class. These questions predominate over the questions affecting individual Class members. These common legal and factual questions include, but are not limited to, the following:

- whether Banner Health engaged in the wrongful conduct alleged herein;
- whether Banner Health owed a duty to Plaintiff and members of the Class to adequately protect their medical, financial, and personal information and to provide timely and accurate notice of the data breach to Plaintiff and the Class;
- whether Banner Health breached its duties to Plaintiff and the Class by failing to provided adequate data security, and whether Banner breached its duty to Plaintiff and the Class by failing to provide timely and accurate notice to Plaintiff and the Class about the breach;
- whether Banner violated federal and state laws, such as HIPAA, thereby breaching its duties to Plaintiff and the Class;
- whether Banner Health knew or should have known that its computer and network systems were vulnerable to attack from hackers;
- whether Banner's conduct, including its failure to act, resulted in or was the proximate cause of the breach of its computer and network systems, resulting in the loss of patients' medical, financial, and personal information;

- whether Banner Health wrongfully failed to inform Plaintiff and members of the Class that it did not maintain computer software and other security procedures sufficient to reasonably safeguard consumer financial and personal data; and whether Banner Health failed to inform Plaintiff and the Class of the data breach in a timely and accurate manner;
- whether Banner Health wrongfully waited for nearly a month after discovery the data breach to inform Plaintiff and Class members that their sensitive and personal information was exposed in the cyberattack;
- whether Plaintiff and members of the Class suffered injury as a proximate result of Banner Health's conduct or failure to act; and
- whether Plaintiff and the Class are entitled to recover damages, equitable relief, and other relief, and the extend of the remedies that should be afforded to Plaintiff and the Class.

COUNT I

Negligence

(Individually and on Behalf of the Class)

54. Plaintiff realleges and incorporates all previous allegations.

55. Banner required Plaintiff and Class Members to submit sensitive personal, medical, and financial information order to obtain services.

56. Banner Health owed a duty to Plaintiff and the Class to maintain confidentiality and to exercise reasonable care in safeguarding and protecting their medical, financial, and personal information in Banner's possession from being compromised by unauthorized persons. This duty included, among other things, designing, maintaining, and testing Banner's security systems to ensure that Plaintiff's and Class members' medical, financial, and personal information in Banner's possession was adequately protected.

57. Banner further owed a duty to Plaintiff and Class members to implement processes that would detect a breach of its security system in a timely manner and to timely act upon warnings and alerts, including those generated by its own security systems.

58. Banner owed a duty to Plaintiff and members of the Class to provide security consistent with industry standards and requirements, to ensure that its computer systems and networks, and the personnel responsible for them, adequately protected the medical, financial, and personal information of Plaintiff and members of the Class whose confidential data Banner obtained and maintained.

59. Banner Health owed a duty to timely and accurately disclose to Plaintiff and members of the Class that their medical, financial, and personal information had been or was reasonably believed to have been compromised. Timely disclosure was required, appropriate, and necessary so that, among other things, Plaintiff and members of the Class could take appropriate measures to avoid identity theft if possible.

60. Banner knew, or should have known, of the risks inherent in collecting and storing the medical, financial, and personal information of Plaintiff and members of the Class and of the critical importance of providing adequate security of that information.

61. Banner's conduct created a foreseeable risk of harm to Plaintiff and members of the Class. This conduct included but was not limited to Banner's failure to take the steps and opportunities to prevent and stop the data breach as described in this Complaint. Banner's conduct also included its decision not to comply with industry standards for the safekeeping and maintenance of the medical, financial, and personal information of Plaintiff and Class members.

62. Banner acted with wanton disregard for the security of Plaintiff and Class Members' personal information. Banner knew or should have known that it had inadequate computer systems and data security practices to safeguard such information,

and Banner knew or should have known that hackers were attempting to access the personal information in health care databases, such as Banner's.

63. To the extent a "special relationship" is required as between Banner, on the one hand, and Plaintiff and Class members, on the other hand, a "special relationship" exists between Banner and the Plaintiff and Class Members. Banner entered into a "special relationship" with the Plaintiff and Class Members whose personal information was requested, collected, and received by Banner as a prerequisite to rendering services. A "special relationship" also exists between Banner, on the one hand, and Plaintiff and Class members, on the other hand, because Banner is a provider of health and health plan services and thus stands in a fiduciary or quasi-fiduciary relationship with Plaintiff and Class Members. Banner entered into a "special relationship" with Plaintiff and Class Members by placing their personal information on Banner's computer servers – information that Plaintiff and Class Members had been required to provide to Banner. Furthermore, Banner also created a "special relationship" with Plaintiff and Class Members who provided their information to Banner by playing a large in role in creating and maintaining centralized computer systems and data security practices that were used for storage of all of Banner customers' personal information.

64. Banner breached the duties it owed to Plaintiff and members of the Class by failing to exercise reasonable care and implement adequate security systems, protocols, and practices sufficient to protect the medical, financial, and personal information of Plaintiff and members of the Class, as identified above. This breach was a proximate cause of injuries and damages suffered by Plaintiff and Class members.

COUNT II

Negligence *Per Se*

(Individually and on behalf of the Class)

65. Plaintiff realleges and incorporates all previous allegations.

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

67. Pursuant to HIPAA (42 U.S.C. § 1302d *et seq.*), Banner had a duty to implement reasonable safeguards to protect Plaintiff's and Class Members' personal information.

68. Pursuant to the Gramm-Leach-Bliley Act (15 U.S.C. § 6801), Banner had a duty to protect the security and confidentiality of Plaintiff's and Class Members' personal information.

69. Pursuant to Arizona state law, Banner had a duty to Plaintiff and Class Members to implement and maintain reasonable security procedures and practices to safeguard Plaintiff's and Class Members' personal information. *See* ARIZ. REV. STAT. § 44-7501; ARIZ. REV. STAT. § 20-2113.

70. Banner breached its duties to Plaintiff and Class Members under the Federal Trade Commission Act (15 U.S.C. § 45), HIPAA (42 U.S.C. § 1302d *et seq.*), GrammLeach-Bliley Act (15 U.S.C. § 6801), and the Arizona data and insurance information security statutes, (ARIZ. REV. STAT. § 44-7501; ARIZ. REV. STAT. § 20-2113), by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' personal information.

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

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

73. The injury and harm suffered by Plaintiff and Class Members was the reasonably foreseeable result of Banner's breach of its duties. Banner knew or should

have known that it was failing to meet its duties, and that its breach would cause Plaintiff and Class Members to experience the foreseeable harms associated with the exposure of their personal information.

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

COUNT III

Negligent Misrepresentation

(Individually and on Behalf of the Class)

75. Plaintiff realleges and incorporates all previous allegations.

76. Banner negligently and recklessly misrepresented material facts pertaining to the sale of health benefits services to Plaintiff and Class Members by representing that it would maintain adequate data privacy and security practices and procedures to safeguard Plaintiff's and Class Members' personal and sensitive information from unauthorized disclosure, release, data breaches, and theft.

77. Banner negligently and recklessly misrepresented material facts pertaining to the sale of health benefits services to Plaintiff and Class Members by representing that they did and would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of Plaintiff's and Class Members' personal information.

78. Because of the inadequacy of their security systems and data protection systems, Banner either knew or should have known that their representations were not true.

79. In reliance upon these misrepresentations, Plaintiff and Class Members purchased health benefits services from Banner.

80. Had Plaintiff and Class Members, as reasonable persons, known of

Banner's inadequate data privacy and security practices, or that Banner was failing to comply with the requirements of federal and state laws pertaining to the privacy and security of personal information, they would not have purchased health benefits services from Banner, and would not have entrusted their personal information to Banner.

81. As direct and proximate consequence of Banner's negligent misrepresentations, Plaintiff and Class Members have suffered the injuries alleged herein.

COUNT IV

Unjust Enrichment

(Individually and on Behalf of the Class)

82. Plaintiff realleges and incorporates all previous allegations.

83. Plaintiff and Class Members conferred a monetary benefit on Banner in the form of monies paid for the purchase of health benefits services.

84. Banner appreciated or had knowledge of the benefits conferred upon them by Plaintiff and Class Members.

85. The monies for health benefits services that Plaintiff and Class Members paid (directly or indirectly) to Banner were supposed to be used by Banner, in part, to pay for the administrative costs of reasonable data privacy and security practices and procedures.

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

87. Under principals of equity and good conscience, Banner should not be permitted to retain the money belonging to Plaintiff and Class Members because Banner failed to implement (or adequately implement) the data privacy and security practices and

procedures that Plaintiff and Class Members paid for and that were otherwise mandated by HIPAA regulations, federal, state and local laws, and industry standards.

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

COUNT V

Violation of the Arizona Consumer Fraud Act,

ARIZ. REV. STAT. §§44-1521, *et seq.* ("ACFA")

(Individually and on behalf of the Class)

89. Plaintiff realleges and incorporates all previous allegations.

90. Plaintiff Clark brings this claim on behalf of herself and the Class.

91. This cause of action is brought pursuant to the ACFA, which provides in pertinent part:

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

Id. § 44-1522.

92. Plaintiff Clark and members of the Class are "persons" as defined by ARIZ. REV. STAT. § 44-1521(6), Banner provides "services" as that term is included in the definition of "merchandise" under ARIZ. REV. STAT. § 44-1521(5), and Banner is engaged in the "sale" of "merchandise" as defined by ARIZ. REV. STAT. § 44-1521(7).

93. Banner engaged in deceptive and unfair acts and practices, misrepresentation, and the concealment, suppression, and omission of material facts in connection with the sale and advertisement of "merchandise" (as defined in the ACFA) in violation of the ACFA, including but not limited to the following:

- failing to maintain sufficient security to keep Plaintiff's and Class Members' confidential medical, financial, and personal data from being hacked and stolen;
- misrepresenting material facts to the Class, in connection with the sale of health benefits services, by representing that they would maintain adequate data privacy and security practices and procedures to safeguard Class Members' personal information from unauthorized disclosure, release, data breaches, and theft;
- misrepresenting material facts to the Class, in connection with sale of health benefits services, by representing that Banner did and would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of Class Members' personal information;
- failing to disclose the data breach to Class Members in a timely and accurate manner, in violation of ARIZ. REV. STAT. § 44-7501; and
- failing to take proper action following the data breach to enact adequate privacy and security measures and protect Class Members' personal information from further unauthorized disclosure, release, data breaches, and theft.

94. In addition, Banner's failure to disclose that its computer systems were not well-protected and that Plaintiff's and Class members' sensitive information was vulnerable and susceptible to intrusion and cyberattacks constitutes deceptive and/or unfair acts or practices because Banner knew such facts would (a) be unknown to and not easily discoverable by Plaintiff Clark and the Class; and (b) defeat Plaintiff Clark's and Class members' ordinary, foreseeable and reasonable expectations concerning the security of Banner's computer servers.

95. Defendant intended that Plaintiff and the Class rely on its deceptive and unfair acts and practices, misrepresentations, and the concealment, suppression, and omission of material facts, in connection with Banner's offering of medical services and incorporating Plaintiff's and Class members' sensitive information on its computer servers, in violation of the AFCA.

96. Banner also engaged in unfair acts and practices, in connection with the sale of health benefits services by failing to maintain the privacy and security of Class Members' personal information, in violation of duties imposed by and public policies reflected in applicable federal and state laws, resulting in the data breach. These unfair acts and practices violated duties imposed by laws including the Federal Trade Commission Act (15 U.S.C. § 45), HIPAA (42 U.S.C. § 1302d *et seq*.), and the Gramm-Leach-Bliley Act (15 U.S.C. § 6801), and the Arizona Insurance Information and Privacy Protection Act (ARIZ. REV. STAT. § 20-2113).

97. Banner's wrongful practices occurred in the course of trade or commerce.

98. Banner's wrongful practices were and are injurious to the public interest because those practices were part of a generalized course of conduct on the part of Banner that applied to all Class members and were repeated continuously before and after Banner obtained confidential medical, financial, and personal data concerning Plaintiff and Class members. All Class members have been adversely affected by Banner's conduct and the public was and is at risk as a result thereof.

99. As a result of Banner's wrongful conduct, Plaintiff and Class members were injured in their business or property in that they never would have allowed their sensitive and personal data – property that they have now lost – to be provided to Banner if they had been told or knew that Banner failed to maintain sufficient security to keep such data from being hacked and taken by others.

100. Banner's unfair and/or deceptive conduct proximately caused Plaintiff's and Class members' injuries because, had Banner maintained the sensitive information with adequate security, Plaintiff and the Class members would not have lost it.

101. Plaintiff and the Class seek actual damages, compensatory, punitive damages, injunctive relief, and court costs and attorneys' fees as a result of Defendants' violations of the AFCA.

PRAYER FOR RELIEF

Plaintiff, on behalf of herself and the Class, respectfully requests that the Court grant the following relief:

A. Certify this case as a class action pursuant to FED. R. CIV. P. 23(a), (b)(2) and (b)(3), and, pursuant to FED. R. CIV. P. 23(g), appoint Plaintiff as Class representative and her counsel as Class counsel.

B. Award Plaintiff and the Class appropriate monetary relief, including actual damages, restitution, and disgorgement.

C. Award Plaintiff and the Class equitable, injunctive and declaratory relief as maybe appropriate. Plaintiff, on behalf of the Class, seeks appropriate injunctive relief designed to ensure against the recurrence of a data breach by adopting and implementing best security data practices to safeguard subscribers' medical, financial, and personal information and that would include, without limitation, an order and judgment directing Banner Health to (1) encrypt all sensitive medical, financial, and personal data in all places in which that data is stored; (2) comply with all applicable industry standards for data security and protection; (3) comply with laws and standards protecting medical data; (4) directing Banner to provide to Plaintiff and Class members extended credit monitoring services and services to protect against all types of identity theft, especially including medical identity theft, to protect them against the ongoing harm presented by

the data breach, and (5) requiring Banner to provide elevated credit monitoring services to minor and elderly Class members who are more susceptible to fraud and identity theft.

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

E. Award Plaintiff and the Class reasonable attorneys' fees and costs as allowable.

F. Award Plaintiff and the Class such other favorable relief as allowable under law or at equity.

DATED this 9th day of August, 2016.

GALLAGHER & KENNEDY, P.A.

By */s/ Lincoln Combs*

Paul L. Stoller
Lincoln Combs
2575 E. Camelback Road, Suite 1100
Phoenix, Arizona 85016-9225
As local counsel for:

Benjamin F. Johns
Andrew W. Ferich
CHIMICLES & TIKELLIS LLP
One Haverford Centre
361 Lancaster Avenue
Haverford, PA 19041
(610) 642-8500
bfj@chimicles.com
awf@chimicles.com

Counsel for Plaintiff and the Putative Class

5564384v3/99-8684