Paul L. Stoller (Bar No. 016773)
Lincoln Combs (Bar No. 025080)
GALLAGHER & KENNEDY, P.A.
2575 East Camelback Road
Phoenix, Arizona 85016-9225
Telephone: (602) 530-8000
Facsimile: (602) 530-8500
E-mails: paul.stoller@gknet.com
lincoln.combs@gknet.com

As local counsel on behalf of:

Hadley L. Matarazzo
Kathryn Bruns
FARACI LANGE, LLP
28 East Main Street, Suite 1100
Rochester, New York 14614
Telephone: (585) 325-5150
Email: hmatarazzo@faraci.com
kbruns@faraci.com

Counsel for Plaintiffs and the Putative Class (*pro hac vice* applications to be filed)

UNITED STATES DISTRICT COURT

FOR THE DISTRICT OF ARIZIONA

JACQUELINE DUHAME a single woman; and EMILY RYANS, a single woman, Plaintiffs, v. BANNER HEALTH, an Arizona Corporation, and BANNER – UNIVERSITY MEDICAL GROUP, an Arizona Corporation, Defendants.	No. **CLASS ACTION COMPLAINT** **AND** **DEMAND FOR JURY TRIAL**

Plaintiffs, on behalf of themselves and all other persons and entities similarly situated, allege as follows:

1. This is a class action lawsuit brought on behalf of Plaintiffs and all other persons similarly situated against Banner Health and Banner – University Medical Group ("Banner") for its failure to adequately protect the confidential, private personal and health information of patients, members, customers, and healthcare providers.

2. The personally identifying information ("PII") and protected health information ("PHI") provided to Banner by Plaintiffs and other Class members, to be held in the strictest confidence, includes names, dates of birth, addresses, physician names, dates of service, clinical information, health insurance information, and social security numbers. Banner has collected and stored all of this information for year.

3. Banner has also received information from its point-of-sales ("POS") systems as to payment cards for customers, including cardholder names, card number, expiration date, and internal verification codes that is routed through Banner's payment processing systems.

4. Banner received this information from Plaintiffs and the Class members understanding that it is both valuable and vulnerable to cyber criminals. The data collected and stored by healthcare providers and health insurance companies like Banner are among the most highly sensitive personally identifiable information. Thus, healthcare companies like Banner bear crucial responsibility to protect such data from compromise and theft.

5. And, there is a significant threat of compromise. The warnings of threats targeting the healthcare industry are nearly ubiquitous from government and law enforcement agencies and cybersecurity experts. These risks are well known; thus, as a company in the business of healthcare that possesses such information, Banner assumed duty to protect that information against these known risks, to take affirmative steps to thwart preventable attacks, and to minimize the risks or damage in the event of successful penetration of their information systems.

6. Indeed, because of these significant risks, healthcare services companies, including Banner, are required to protect their customers' PII and PHI by adopting and implementing data security regulations and standards, including those set forth under the Health Insurance Portability and Accountability Act ("HIPAA"), the Health Information Technology for Economic and Clinical Health Act ("HITECH Act"), applicable state law, and common law.

7. To that end, Banner repeatedly promised to Plaintiffs, patients at their facilities, members and beneficiaries of its healthcare plans, and physicians who provided them with PII and PHI that Banner would safeguard and protect that information from disclosure – including in its privacy policies.

8. In June 2016, hackers obtained access to Banner's POS systems at food and beverage outlets in Banner facilities. Through that access, hackers were able to access and to obtain Payment Card Information for customers at those food and beverage outlets during the period from June 23, 2016 to July 7, 2016.

9. Unbelievably for this day and age, Banner failed to separate and segregate its systems and servers containing the PII and PHI of patients, healthcare plan members, and providers from its POS systems. As a result, the hackers of Banner's POS systems were able to use the access they gained through those systems to obtain access to Banner's broader information systems and specifically to obtain the PII and PHI of upwards of 3.7 million people.

10. As a result of these failings by Banner, described in greater detail below, Plaintiffs and other class members have suffered great harm and face a certainly impending risk of future harm. The PII and PHI exposed by Banner in this case is essentially a complete package for anyone seeking to steal someone's identity. Additionally, in clear contravention of the requirements of HIPAA, Banner failed to take essential steps to protect the PHI of Class Members from precisely this type of foreseeable hack.

11. Plaintiffs, therefore, bring this action seeking redress and compensation for the harm caused to them and the other class members by virtue of the Banner's failures to protect their information.

PARTIES, JURISDICTION, AND VENUE

12. Plaintiff Jacqueline Duhame is a resident of Maricopa County, Arizona.

13. Plaintiff Emily Ryan is a resident of Maricopa County, Arizona.

14. Banner Health is a not-for-profit corporation organized under the laws of the State of Arizona. Banner Health's headquarters and principal place of operations are in Maricopa County, Arizona.

15. Banner – University Medical Group is a not-for-profit corporation organized under the laws of the State of Arizona. Banner – University Medical Group's headquarters and principal place of operations are in Maricopa County, Arizona.

16. Jurisdiction is proper in this Court pursuant to the Class Action Fairness Act, 28 U.S.C. § 1332(d), because the aggregate amount in controversy exceeds $5,000,000, exclusive of costs and interests, and some Class members are citizens of states different from Banner's home state.

17. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(b) because Banner resides in this district and regularly conduct business in this district, a substantial part of the events or omissions giving rise to these claims occurred in this district, and Banner caused harm to Class members residing in this district.

FACTS

18. Banner owns and operates numerous healthcare facilities across seven states, including Arizona, Alaska, California, Colorado, Nebraska, Nevada, and Wyoming. These include 29 hospitals as well as long-term care centers, outpatient surgery centers, family clinics, home care and hospice services, pharmacies, and a nursing registry. Banner – University Medical Group operates multiple university hospitals and healthcare facilities in Arizona.

19. On information and belief, for years, Banner has collected PII and PHI from its patients, members of its healthcare plans, and healthcare providers at its facilities and in its healthcare plan networks.

20. As described above, the PII and PHI includes names, dates of birth, addresses, physician names, dates of service, clinical information, health insurance information, and social security numbers.

21. In collecting PII and PHI from patients, members of its healthcare plans, and healthcare providers, Banner explicitly and implicitly promises, represents, and warrants that it will respect and ensure the privacy and confidentiality of that information.

22. For example, in its Notice of Privacy Practices for Banner Health, Banner represents that it "is committed to protecting the confidentiality of information about you, and is required by law to do so." The most recent version of this notice was effective starting September 23, 2103. On information and belief, Banner had prior versions of this confidentiality notice beginning at least as early as 1996 after HIPAA was enacted and each such version of the notice contained a similar commitment to protect the PII and PHI of patients and healthcare plan members and beneficiaries.

23. On its website (www.bannerhealth.com), under Privacy Practices for Banner Health, it states, "Banner is committed to protecting the confidentiality of information about you, and is required by law to do so."

24. Similar representations to maintain the privacy and confidentiality of patient information exist in Banner's contracts with its patients. For example, in its Behavioral Health Clients Rights document, Banner represents that the patient has the right "[t]o have the client's information and records kept confidential and released only as permitted under R9-20-211(A)(3) and (B)." The same document provides that the patient has the right "[t]o privacy in treatment …."

25. Banner, as a "Covered Entity" under HIPAA, has special obligations to protect the PHI of its patients and members of its healthcare plans under HIPAA. These obligations include compliance with both the "Privacy Rule" and the "Security Rule." The Privacy Rule requires Banner to have administrative, physical, and technical safeguards to ensure that protection of PHI. The Security Rule requires Banner to protect against reasonably anticipated threats to the security of PHI.

26. Banner is also prohibited, under the Federal Trade Commission Act, 14 U.S.C. § 45, from engaging in unfair and deceptive acts or practices. The FTC has determined that a company's failure to maintain reasonable and appropriate data security

for PII is an "unfair practice" under the Act. Thus, Banner was obligated under the Act to maintain reasonable and appropriate data security for the PII and PHI of Plaintiffs and Class members.

27. In addition to its existing duties to protect the PII and PHI of Plaintiffs and Class members from cyber attackers, Banner knew or should have known that it was a high target for such criminals. It further knew or should have known that its data security systems were inadequate to prevent the type of attack it ultimately suffered.

28. Banner suffered a data breach in or about February 2014. At that time, Banner exposed the PII of approximately 50,000 people by placing their social security numbers and/or Medicare identification numbers on address labels for Banner's quarterly magazine sent to members of one of its healthcare networks. As a company that has already exposed sensitive PII of customers, Banner should have been acutely aware of the need to protect sensitive and confidential patient and customer information.

29. Well before the attack, cybersecurity experts and healthcare industry experts had long and widely announced that healthcare companies were prime targets for cyber criminals.

30. In December 2012, the Ponemon Institute, in its Third Annual Benchmark Study on Patient Privacy and Data Security, found that nearly 33 percent of all healthcare data breaches involved cyberattacks.[1] It further found that the healthcare companies themselves generally "agree[d] that patients are at a greater risk of financial identity theft if their records are lost or stolen."[2]

31. In April 2014, the Federal Bureau of Investigation (FBI) Cyber Division issued a "Private Industry Notification" to the healthcare industry and stated that "the health care industry is not technically prepared to combat against cyber criminals' basic cyber intrusion tactics, techniques and procedures (TTPs), much less against more

[1] Ponemon Institute, Third Annual Benchmark Study on Patient Privacy & Data Security, at 9 (Dec. 2012), *available at* http://lpa.idexpertscorp.com/acton/attachment/6200/f-0033/1/-/-/-/-/file.pdf.
[2] *Id.* at 12.

advanced persistent threats (APTs). The health care industry is not as resilient to cyber intrusions compared to the financial and retail sectors, therefore the possibility of increased cyber intrusions is likely."

32. Within months, Community Health Systems, Inc., one of the nation's largest for-profit healthcare providers, suffered a data breach affecting 4.5 million customers. Shortly thereafter, the FBI warned healthcare companies that hackers were targeting them, stating that it "has observed malicious actors targeting healthcare related systems, perhaps for the purpose of obtaining Protected Healthcare Information (PHI) and/or Personally Identifiable Information (PII)."[3]

33. As Dave Kennedy, chief executive of information security firm TrustedSEC, has explained, cyber criminals target healthcare companies precisely because they maintain large quantities of data that has significant resale value in black markets and because generally their security practices are lax and less sophisticated than those of other industries. Mr. Kennedy also noted that "[h]ealth organizations sometimes rely on legacy systems, and some have not invested in cybersecurity at a rate that matches the urgency of the threats they face. The medical industry is years behind other industries when it comes to security."[4]

34. And, over the past two years, the data breaches of Premera, Anthem, and Excellus/Blue Cross Blue Shield have splashed the headlines.

35. Banner was on notice that it was a prime target for cyber attackers and that it had an obligation to implement reasonable safeguards and security measures for the protection of the PII and PHI of Plaintiffs and Class members that it possessed.

---

[3] Jim Finkle, FBI warns healthcare firms that they are targeted by hackers, Reuters (Aug. 2014, 4:32 PM), http://www.reuters.com/article/2014/08/20/us-cybersecurity-healthcare-fbi-idUSKBN0GK24U20140820.

[4] Andrea Peterson, 2015 is Already the Year of the Health-Care Hack—and It's Only Going to Get Worse, Wash. Post, Mar. 20, 2015, *available at* http://www.washingtonpost.com/blogs/the-switch/wp/2015/03/20/2015-is-already-the-year-of-the-health-care-hack-and-its-only-going-to-get-worse/ (last accessed Aug. 6, 2016).

36. Notwithstanding its representations, promises, and duties to protect and to safeguard the PII and PHI it collects and stores from Class members and the knowledge that it was a prime target for cyber attackers, Banner has failed to take appropriate steps to ensure the security of that information.

37. In particular, despite prior publicly-known data breaches by which hackers accessed PII through the hacking of POS systems, Banner failed to segregate the systems that maintained the PII and PHI of Class Members from its systems that managed the POS systems. As a result, hackers who exposed vulnerabilities in Banner's POS systems had the ability to access Banner's other information systems, including those that contain Class member PII and PHI.

38. Indeed, beginning on or about June 17, 2016, unknown hackers exposed vulnerabilities in Banner's POS systems at food and beverage sales sites at approximately 20 Banner locations in Arizona, five locations in Colorado, one location in Alaska, and one location in Wyoming. As a result, the hackers were able to capture payment card information for transactions that took place at those locations between June 23, 2016 and July 7, 2016.

39. Banner learned of the breach of its POS systems on July 7, 2016.

40. On information and belief, including based on the press releases and public statements by Banner, the hackers who breached Banner's POS system were able to access Banner's larger information systems via its POS system, which in turn gave the hackers access to patient information, health-plan member and beneficiary information, and information about healthcare providers, including PII and PHI of those individuals. Patient information that was accessed includes names, dates of birth, addresses, physician's names, dates of service, claims information, health insurance information, and social security numbers. The healthcare provider information that was exposed includes names, addresses, dates of birth, social security numbers, and "other identifiers," according to Banner.

41. On July 13, 2016, Banner discovered that the hackers had accessed the PII and PHI of patients, health-plan members and beneficiaries, and healthcare providers by accessing the information through the vulnerabilities exposed in the POS system.

42. Three weeks later, on August 3, 2016, Banner announced that its systems had been hacked and that the payment card information, PII, and PHI of 3.7 million Banner patients, health-plan members and beneficiaries, healthcare providers, and customers whose credit cards were used during the two-weeks Banner's POS system had been hacked.

43. On or about August 3, 2016, Banner began notifying affected individuals of the breach. Banner's notification campaign appears to have two components: internet notice and mailed notice.

44. On or about August 3, 2016, Banner established a website at www.bannersupports.com at which it posted a notice of the breach. On that site and in the notice, it directs potentially affected persons to call a 1-855 telephone number to obtain information "[i]f you do not receive a letter by September 9, 2016 and you remain concerned that you are affected …." Similarly, in its August 3 press release, posted on Banner's business website (www.bannerhealth.com), Banner stated: "Customers with questions can call 1-855-223-4412, from 7 a.m. to 7 p.m. Pacific Time, seven days a week."

45. Banner also purportedly began mailing letters to affected individuals on August 3, 2016. However, on information and belief, Banner did not mail notices to all of the 3.7 million affected persons at that time; rather, it is sending out notice to affected individuals in groups (or batches). Plaintiffs do not know how many groups (or batches) of notices Banner intends to send out. But, on information and belief, Banner's mailing plan includes mailing some groups (or batches) of notices out as late as September.

46. The net result of this notice scheme is that a substantial portion and substantial number of Class members will not be receive notice until anywhere from one

to two months after Banner begins mailed notice, and two to three months after the breach itself happened.

47. Moreover, although Banner knows the identity of all affected individuals, it is not disclosing to affected individuals whether their information may have been accessed by hackers until such time as it actually sends notice to those individuals. Although Banner's website and press release identify a 1-855 telephone number for potentially affected individuals to call, the Banner representatives answering the calls can only answer questions regarding affected individuals to whom Banner has already sent notice. In particular, the Banner representative does not possess the list of all affected individuals – only those persons to whom Banner has actually already sent notice. As a result, a Class member whose PII and PHI has been hacked but to whom Banner has not yet sent mailed notice (due to its process of sending the notice in groups) is told that the Banner representative cannot tell him or her whether he or she is at risk because the representative does not have the list of all affected individuals. In other words, although Banner knows the identity of the affected individuals and has publicly told them to call its 1-855 telephone number to get information, it will not tell those individuals whether their information was part of the breach unless it has already sent them mailed notice – effectively precluding a large portion of the Class from timely learning that their PII and PHI is at risk.

48. As a result of Banner's actions, Plaintiffs and Class members have suffered, or are at imminent risk of further suffering, identity theft and medical-identity theft. Indeed, victims whose information is stolen in a data breach face significantly greater risk of having their identity stolen than in the absence of such a breach. According to a 2014 survey by National Consumers League, victims of data breaches now face a one-in-three chance of having their identity stolen; this is up from one in nine in 2010.[5]

[5] National Consumers League, The Consumer Data Insecurity Report: Examining the Data Breach – Identity Fraud in Four Major Metropolitan Areas, *available at* http://www.nclnet.org/datainsecurity_report (last accessed Aug. 7, 2016).

Comparatively, the general population (which includes victims of data breaches) has only about a seven percent chance of having identity theft.[6]

49. The information that Banner maintained from Plaintiffs and Class members includes some of the most important and useful information to identity thieves and hackers.

50. Social security numbers are particularly among the worst kind of personal information to have stolen. They can be used by identity thieves in a variety of ways and are difficult for an affected individual to change.

51. One significant risk to victims whose social security number has been stolen is credit-identity theft. As the Social Security Administration has warned, identity thieves can use an individual's social security number and good credit score to apply for credit in the name of the victim.[7] This type of fraud can go undetected for months or even years.

52. Identity thieves can also use stolen social security numbers to file fraudulent tax returns, file for unemployment benefits, or apply for a job using a false identity. These fraudulent activities are difficult to detect until after the damage is done. Victims often do not learn that a fraudulent tax return has been filed until the IRS rejects their filing of an authentic tax return. The use of stolen social security numbers for fraudulent unemployment benefits are often not discovered for long periods of time, sometimes not until law enforcement notifies the employer of suspected fraud.

53. Complicating the damages caused by social security number theft and use is that it is difficult to change or cancel a stolen social security number. Obtaining a new social security number requires significant paperwork and evidence of actual misuse. Thus, it is nearly impossible to obtain a new social security number as a preventative

---

[6] Susan Ladika, Data Breaches Pose a Greater Risk, July 28, 2014, *available at* http://www.foxbusiness.com/features/2014/07/23/study-data-breaches-pose-greater-risk.html (last accessed Aug. 7, 2016).

[7] Social Security Administration, Identity Theft and Your Social Security Number, *available at* http://www.ssa.gov/pubs/EN-05-10064.pdf (last visited Aug. 6, 2016).

measure because the affected person must show that there is actual, ongoing fraud with his or her existing social security number to obtain a new one.

54. Even then, obtaining a new social security number may not prevent the harm to the victim's credit identity. According to Julie Ferguson of the Identity Theft Resource Center, "The credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[8]

55. For minors whose social security number and personal information is compromised, there are significant additional problems. Unlike adults who can take affirmative steps to monitor their credit, minors typically do not have established credit to monitor. For that reason, most credit monitoring companies do not even offer credit monitoring services for minors. As a result, most minors cannot take action to freeze or protect their credit until they are 18. For many minors that can mean years or even more than a decade to take any action to protect themselves from identity theft and harm to their credit. By that time, the damage can be absolutely devastating with a new adult's complete identity stolen and used for years.

56. Additionally, where, as here, the hackers and identity thieves have accessed and stolen social security numbers and health care information, they can use that information to obtain medical care in someone else's name. Medical-identity theft is a rising form of identity theft and has begun to get more attention in the wake of breaches of several major healthcare insurance companies.

57. The FTC defines medical-identity theft as a cyber attacker "us[ing] [a victim's] name or health insurance numbers to see a doctor, get prescription drugs, file

[8] Victims of Social Security Number Theft Find It's Hard to Bounce Back, NPR, Brian Naylor, Feb. 9, 2015, *available at* http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft (last visited Aug. 6, 2016).

claims with [the victim's] insurance provider, or get other care."[9] Medical-identity theft can later affect the victim's treatment, insurance and payment records, and credit.[10]

58. The February 2015 Fifth Annual Study on Medical Identity Theft by the Ponemon Institute found that "[u]nlike credit card fraud, victims of medical identity theft can suffer significant financial consequences. Sixty-five percent of medical identity theft victims in our study had to pay an average of $13,500 to resolve the crime."[11] An earlier study by Ponemon found that the "average total cost" of such theft is "about $20,000" per incident.[12] That earlier study also concluded that a majority of medical-identity-theft victims were forced to pay out-of-pocket costs for healthcare they did not receive in order to regain coverage. Almost half of medical-identity-theft victims lose their healthcare coverage as a result of the theft; and nearly one-third incurred increased insurance premium cost; a staggering 40 percent were never able to resolve their identity theft.[13] Further, the February 2015 Ponemon study found that 65 percent of medical-identity-theft victims spend an average of 200 hours to sort out the mess created by the medical identity theft, including working with insurers and healthcare providers to secure their credentials, verifying personal information, and ensuring their records are accurate.[14] And, only 10 percent "report achieving a completely satisfactory conclusion of the incident."

59. Fraudulent medical treatment can have additional non-financial impacts on victims. For example, Deborah Peel, executive director of Patient Privacy Rights, has

---

[9] Medical Identity Theft, Federal Trade Commission, https://www.consumer.ftc.gov/articles/0171-medical-identity-theft (last visited Aug. 6, 2016).

[10] *Id.*

[11] Ponemon Institute, Fifth Annual Study on Medical Identity Theft (Feb. 2015), *available at* http://medidfraud.org/wp-content/uploads/2015/02/2014_Medical_ID_Theft_Study1.pdf (last visited Aug. 6, 2016).

[12] CNET, *Study: Medical identity theft is costly for victims*, http://www.cnet.com/news/study-medical-identity-theft-is-costly-for-victims/ (last visited Aug. 6, 2016).

[13] *Id.*

[14] Ponemon Institute, Fifth Annual Study on Medical Identity Theft, note 5, *supra*.

described lasting effects on healthcare as a result of a person's medical history containing false information, such as victims being given the wrong blood type or administered improper medicines due to the wrong information being in their records.[15]

60. As Pam Dixon, executive director of the World Privacy Forum, stated: "When 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 qualitatively and quantitatively different than what is typically possible when you lose your credit card or Social Security number."[16]

61. Victims of data breaches involving medical information, such as this, also face imminent risk of health insurance discrimination. Because their medical information becomes contaminated, victims face denial of coverage, improper "redlining," and denial or difficulty obtaining disability or employment benefits. This risk is pervasive and widespread. Indeed, most states maintain government agencies that investigate and combat health insurance discrimination, as does the U.S. Department of Health and Human Services' Office of Civil Rights ("OCR").

62. As a result of the foregoing, the information accessed and taken by hackers in the Banner breach is significantly more valuable to the cyber-criminal than that taken in a large credit-card breach. Victims in the latter situation can avoid much of the potential for future harm by cancelling payment cards and obtaining replacements. Even then, fraudulent credit card losses almost always fall on the banks issuing the cards and not the cardholders. The information taken in this breach is difficult, if not impossible, to change—social security number, name, date of birth, medical or clinical information, etc.

63. This type of information is much more valuable to cyber criminals. Martin Walter, senior director at cybersecurity firm RedSeal, has stated that "[PII] and social

---

[15] *See* Peterson, note 4 *supra.*

[16] Jaikumar Vijayan, Premera Hack: What Criminals Can Do With Your Healthcare Data, Christian Science Monitor, Mar. 20, 2015, *available at* http://www.csmonitor.com/World/Passcode/2015/0320/Premera-hack-What-criminals-can-do-with-your-healthcare-data (last visited Aug. 6, 2016).

security numbers are worth more than ten times in price" on the black market as compared to credit card information.[17]

64. This estimate may be low. A recent PricewaterhouseCoopers report stated that an identity theft kit containing health insurance credentials can be worth up to $1,000 on the black market, as compared to stolen credit cards which may sell for $1 each.

65. Banner's notice to victims offers a "Band-Aid," stating that Banner will provide one year of "fraud monitoring." But Banner's offer provides very limited and ineffective protection to Plaintiffs and the Class from the virtually inevitable attempts at identity theft they will face. This "offer," which has become a customary ploy to stave off claims, provides scant protection and is woefully insufficient to address the harm suffered by the victims of Banner's conduct.

66. As a threshold matter, the monitoring offer comes too late for many victims. Banner's delayed notice to a substantial number of Class members (who Banner will not tell they are affected even if they call before being mailed notice) means that it will be 60 to 90 or more days after their PII and PHI was stolen before many Class members will even have the opportunity to use these services (or even know their PII and PHI is at risk). By then, Plaintiffs' and class members' PII and/or PHI may already have been sold to criminals and identity theft may already have occurred or be well underway.

67. Additionally, the offer requires affirmative action by the victims, the vast majority of whom Banner knows are not likely to actually receive the notice or to sign up.

68. Moreover, the "monitoring" is less than comprehensive. The monitoring offered by Banner only monitors one of the three major credit reporting bureaus – leaving unattended two-thirds of the sources from which identity theft can be detected. Additionally, one year is wholly inadequate for victims whose compromised PII includes

[17] Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers, IT World, Tim Greene, Feb. 6, 2015, *available at* http://www.itworld.com/article/2880960/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last visited Aug. 6, 2016).

an entire package of identity information with social security numbers and dates of birth, and who face substantial risk of identity theft for years after the "monitoring" expires.

69. Banner's proposed customer solutions also do nothing to address the problem of medical-identity theft. To guard against medical-identity fraud, cybersecurity experts suggest that individuals routinely obtain the most recent copies of their medical records and inspect them for discrepancies. But, Banner has done nothing to advise its patients and insurance customers how to obtain and inspect their medical records for fraud to follow best practices identified by security experts; nor has Banner offered to reimburse any costs associated with obtaining medical records or for their review.

70. As a result of Banner's actions, including its knowing failure to implement the necessary steps to protect the PII and PHI that was entrusted to it, the PII and PHI of Plaintiffs and the members of the Class has been exposed and made available and accessible to hackers and, thus, to identity thieves.

71. Neither Plaintiffs nor the members of the putative Class authorized Banner to disclose their PII or PHI to the public.

72. Banner's actions, including its knowing failure to implement the necessary steps to protect that PII and PHI, have exposed the Class Members to the potential for identity theft for the remainders of their natural lives. And, Banner's actions have dramatically increased the likelihood that Plaintiffs and Class members will be victims of identity theft.

73. As a result, many Class members have incurred and will incur out-of-pocket expenses either to address or to prevent identity theft or to secure protection against the potential for the identity theft and medical-identity theft to which Banner has exposed them. On information and belief, this includes fees for things such as changing bank accounts, obtaining replacement checks, changing credit cards, obtaining credit reports, phone charges, postage, and the costs of obtaining adequate credit monitoring and identity theft insurance.

74. All of these injuries suffered by the Plaintiffs and Class members are a direct and proximate result of the Banner data breach and include:

a. theft of their PII and PHI;

b. costs associated with the detection and prevention of identity theft and unauthorized use of their PII, and financial, business, banking, and other accounts;

c. costs associated with the detection and prevention of medical-identity theft and unauthorized use of their PHI and insurance accounts;

d. costs associated with time lost addressing and attempting to ameliorate, mitigate, and deal with the actual and future consequences of the Banner data breach, including finding fraudulent filed tax returns, theft of social security payments, fraudulent charges, cancelling credit cards, evaluating the burden and potential benefit of applying for a new social security number, signing up for and purchasing credit monitoring and identity-theft and medical-identity-theft protection services, the imposition of withdrawal and purchase limits on compromised accounts, time spent without access to credit while a new credit card is being issued, and the stress, nuisance, and annoyance of dealing with all issues resulting from the Banner data breach, including additional phishing emails and phone scams;

e. the imminent and certain impending injury flowing from fraud and identify theft posed by their PII and PHI being placed in the hands of unknown third parties;

f. damages to and diminution in value of their PII and PHI entrusted to Banner for the sole purpose of obtaining healthcare, or other services from Banner, with the mutual understanding that Banner would safeguard against theft and take all steps available to prevent access to or misuse of Plaintiffs' and Class members' data by unauthorized third parties;

g. money paid to Banner for healthcare services, or other services because

Plaintiffs and Class members would not have obtained healthcare services, or other services from Banner had Banner disclosed that they lacked adequate systems and procedures to reasonably safeguard customers' PII and PHI;

h. overpayments to Banner for healthcare services, or other services purchased, in that a portion of the price for healthcare services, or other services paid by Plaintiffs and Class members to Banner was for the costs of Banner to take reasonable and adequate security measures to protect PII and PHI, which Banner failed to do; and

i. continued risk to Plaintiffs' and Class members' PII and PHI, which remains in the possession of Banner and which is subject to further breaches so long as Banner fails to undertake appropriate and adequate measures to protect the PII and PHI entrusted to it.

PLAINTIFFS

75. Plaintiff Jacqueline Duhame is a former patient of Banner. As such, she provided her PII/PHI to Banner, which would have included, among other things, her name, date of birth, address, current and former addresses, telephone numbers, email addresses, social security number, and financial information. She also provided her private medical health information and health insurance information to Banner.

76. Ms. Duhame is very sensitive to the potential for identity theft. She is vigilant in protecting her PII and PHI, takes reasonable precautions to keep it out of the public domain.

77. Jacqueline Duhame is a victim of the breach. She received a letter from Banner dated August 3, 2016 informing her that her PII and PHI was involved in a cyber attack on its IT network.

78. To her knowledge, Ms. Duhame is not yet the victim of identity theft. However, she has suffered substantial, irreparable harm by virtue of the fact that her PII and PHI was compromised and disclosed to one or more criminals whose identity

remains unknown, and that her PII and PHI will remain at risk, in the public domain, permanently. Plaintiff Jacqueline Duhame faces imminent risk of harm as a result of the breach.

79. Plaintiff Emily Ryan is a former patient of Banner. As such, she provided her PII and PHI to Banner, which would have included, among other things, her name, date of birth, address, Social Security number, telephone numbers, email addresses, and financial information. She also provided her private medical health information and health insurance information to Banner.

80. Plaintiff Emily Ryan is very sensitive to the potential for identity theft. She is vigilant in protecting her PII and PHI, takes reasonable precautions to keep it out of the public domain.

81. Ms. Ryan has not received Banner's form notice of the breach described above. Nonetheless, she reasonably believes she may be one of approximately 3.7 million victims of the Banner breach because she provided her PII and PHI to Banner in or about September 2015. To her knowledge, Ms. Ryan is not yet the victim of identity theft. However, assuming she is a victim, she has suffered substantial, irreparable harm by virtue of the fact that his/her PII and PHI was compromised and disclosed to one or more criminals whose identity remains unknown, and that her PII and PHI will remain at risk, in the public domain, permanently. If Plaintiff Emily Ryan's PII and PHI was involved in the cyber attack involving Banner's IT network, she faces imminent risk of harm as a result of the breach.

82. Plaintiff Emily Ryan called the posted 1-855 telephone number in Banner's internet notice regarding the breach on or about August 9, 2016. In response to that call, the Banner representative told Ms. Ryan that she could not tell Ms. Ryan whether she was one of the 3.7 million people affected by the breach because Plaintiff Ryan's name was not on the list of individuals to whom notice has already been sent. The representative told Ms. Ryan that Banner is sending notices out in batches and will have all notices out by the end of September.

83. On or about August 12, 2016, Plaintiff Emily Ryan's counsel reached out to Banner's counsel to discuss the fact that potentially affected individuals were unable to determine whether they were affected by calling the 855 number Banner provided or by reviewing Banner's web notice. Banner's counsel discussed the situation with Banner's notification vendor Kroll and reported back to Plaintiff Ryan's counsel on August 15, 2016 that "as of August 11, the names of all affected persons should have been entered into the system, so if someone calls the call center today, the call center should be able to verify whether or not they are in the affected population, even if a notice has not yet been mailed to them."

84. On or about August 22, 2016, Plaintiff Emily Ryan again called the 855 number Banner provided and spoke with someone at the call center. The individual she spoke with at the call center informed Ms. Ryan that she was "not supposed to check the list," but would do so. After allegedly checking the list, the individual informed Plaintiff Emily Ryan that she was not on the list, but that the list only includes people to whom the breach notification letter has been sent. The individual then explained to Ms. Ryan that a letter notifying the caller if she was affected could go out as late as September 9. Ms. Ryan received the same response she got on August 9, 2016. On or about August 23, 2016, Ms. Ryan's minor son, Colin, received the mailed notice dated August 3, 2016 from Banner, indicating that his PII and PHI had been accessed in the breach.

85. Accordingly, Plaintiff Emily Ryan has no means of determining whether her PII and PHI was accessed by hackers in the Banner breach until Banner notifies her by mail that she was affected by the breach – notice that she may not receive until the end of September, as many as 10 weeks after the breach.

CLASS ALLEGATONS

86. Plaintiffs bring this action under Federal Rule of Civil Procedure 23 on behalf of themselves and all persons or entities whose PII, PHI, and financial information existed on Banner's electronic information systems at the time of the foregoing events and all persons who engaged in credit card transactions at affected locations between

June 23, 2016 and July 7, 2016 (the "Class"). Excluded from the Class are Banner, its officers, directors, and legal representatives, the judicial officers and their staff who are assigned to this matters, and the immediate families of the foregoing. Plaintiffs reserve the right to alter, modify, or expand the Class definition based on further information learned through investigation and discovery.

87. Numerosity. Plaintiffs believe that the Class includes millions of individuals. Banner itself has indicated that approximately 3.7 million people are affected by the breach. The Class is so numerous that joinder of all members in a single action is impracticable.

88. Commonality. Common questions of law and fact exist as to all Class members. These common questions predominate over any questions affecting solely individual Class members. The common questions of law and fact may be determined without reference to individual circumstances and apply consistently to every Class member. The common questions of law and fact include, but are not limited to, the following:

a. Whether Banner owed Plaintiffs and the Class a duty of care with respect to the protection of their PII and PHI;

b. Whether Banner breached its obligations to Plaintiffs and the Class with respect to the protection of their PII and PHI;

c. Whether Banner failed to adequately protect the PII and PHI of Plaintiffs and Class members;

d. Whether Banner knew or should have known that its IT systems were vulnerable to hacking through its POS systems;

e. Whether Banner complied with its obligations under the HIPAA Privacy Rule with respect to the PHI of the Class;

f. Whether Banner complied with its obligations under the HIPAA Security Rule with respect to the PHI of the Class;

g. Whether Banner's computer systems and data security practices complied with federal and state laws;

h. Whether Banner engaged in unfair, unlawful, or deceptive practices by failing to safeguard Plaintiffs' and the Class members' PII and PHI properly and/or as promised;

i. Whether Banner acted negligently in failing to safeguard Plaintiffs' and the Class members' PII and PHI;

j. Whether implied contracts or contracts by estoppel existed between Banner, on the one hand, and Plaintiffs and the members of the Class, on the other;

k. Whether Banner's conduct described herein constitutes a breach of its implied contracts or contracts by estoppel with Plaintiffs and the members of the Class;

l. Whether Banner should retain the money paid by Plaintiffs and members of the Class to protect their PII and PHI;

m. Whether Banner complied with its obligations under A.R.S. § 44-7501(A);

n. Whether Banner complied with its obligations to notify Plaintiffs and Class members of the breach as soon as reasonably practical and in a timely manner;

o. Whether Banner owed Plaintiffs and the Class members a fiduciary duty with respect to the protection of their PII and PHI entrusted to Banner;

p. Whether Banner accepted the PII and PHI of Plaintiffs and the Class members with an obligation to hold it in trust, to use it only for limited purposes essential to Banner, and to protect it from disclosure;

q. Whether Banner accepted and even required the PII and PHI from Plaintiffs and the Class members on the understanding that it would undertake reasonable efforts to ensure that the PII and PHI was secure and could not be accessed, viewed, or acquired unless authorized by law;

r. Whether Banner has violated the Constitutional right of privacy of Plaintiffs and the Class members by failing to take adequate steps to protect the PII and PHI and permitting its disclosure;

s. What was the nature and extent of the breach;

t. Whether Banner's actions permitted unauthorized access to the PII and PHI of Plaintiffs and the Class members;

u. Whether Banner was negligent in its failure to protect adequately the PII and PHI of Plaintiffs and the Class members;

v. Whether Banner's conduct was reckless;

w. Whether Banner's offered remedy of credit monitoring to the Class was inadequate to remedy the harm caused by its failure to adequately protect the PII and PHI of the Class;

x. Whether Plaintiffs and the Class members are entitled to compensatory damages against Banner;

y. Whether Plaintiffs and the Class members are entitled to punitive damages against Banner;

z. Whether Plaintiffs and the Class are entitled to affirmative injunctive relief against Banner.

aa. What equitable relief is appropriate to redress Banner's wrongful conduct; and

bb. What injunctive relief is appropriate to redress the imminent and currently ongoing harm faced by Plaintiffs and Class members.

89. Typicality. Plaintiffs' claims are typical of those of the other Class members. Plaintiffs' claims and those of the Class members have a common source and rest on the same legal and remedial theories. Plaintiffs have suffered similar injuries and harm to the other Class members. Plaintiffs have no interests that are adverse to the interests of the other Class members with respect to the claims and issues in this suit.

90. Adequacy. Plaintiffs have a sufficient stake in the litigation to prosecute their claims vigorously on behalf of the Class members, and the named Plaintiffs' interests are aligned with those of the Class members. Plaintiffs have retained competent counsel experienced in class action and data breach litigation to represent them and the Class in this suit.

91. Predominance. The questions of law and fact common to the Class predominate over any questions affecting only individual Class members.

92. Superiority. A class action is superior to all other methods for the fair and efficient adjudication of this controversy. Individual litigation of the claims of the Class members is economically unfeasible and procedurally impractical. The damages suffered by individual Class members are small relative to the costs of independent litigation; thus, the burden and expense of individual litigation make it unlikely that the vast majority of Class members will ever pursue their claims independently. Moreover, if Class members were to pursue their claims independently, the individual cases would overburden the courts and provide the possibility of inconsistent or contradictory judgments. There will be no difficulty in the management of this action that would preclude its maintenance as a class action.

COUNT I

(Negligence)

93. Plaintiffs incorporate herein the allegations in the previous paragraphs.

94. Banner required Plaintiffs and Class members to provide it with confidential and private PII and PHI in order to provide healthcare services or other services to Plaintiffs and Class members.

95. Based on those requirements and in order to obtain services from Banner, Plaintiffs and Class members provided Banner with a massive amount of PII and PHI belonging to Plaintiffs and Class members.

96. Banner collected and stored this data and knew, or should have known, of the risks inherent in collecting and storing the PII and PHI of Plaintiffs and Class members.

97. Banner owed Plaintiffs and all Class members a duty of reasonable care in the handling, maintenance, and security of their PII and PHI. Banner owed, undertook, and/or assumed duties of care to use reasonable means to secure and safeguard this PII and PHI, to prevent disclosure of the information, and to take reasonable measures to guard the information from cyberattacks. These duties include, among others, a responsibility to implement reasonable technical, administrative, and physical security measures to protect the PII and PHI from cyber criminals, ensuring that it could detect, respond to, remedy, and promptly notify affected individuals in the event of a security breach, and maintaining PII and PHI in its networks only as long as necessary and required by law. In particular to this case, Banner had a duty to ensure that the PII and PHI of Plaintiffs and Class members was not accessible through breaches of Banner's POS systems at its food and beverage locations.

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

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

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

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

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

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

99. Through its acts and omissions, including those described above, Banner breached its duty of reasonable care to Plaintiffs and the Class members. Banner negligently maintained systems that were vulnerable to a security breach, and it knew or should have known of these vulnerabilities.

100. Banner acted with wanton disregard for the security of Plaintiffs' and Class members' PII and PHI. Banner knew or should have known that it had inadequate computer systems and data security practices to safeguard such information, and it knew or should have known that hackers were attempting to access the PII and PHI in healthcare systems, such as Banner's systems.

101. As a direct and proximate result of Banner's actions, the PII and PHI of Plaintiffs and the Class have been exposed to cybercriminals who intend to use that information for illegal purposes, including identity theft and medical-identity theft.

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

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

104. As a direct and proximate result of Banner's breaches of it duties, Plaintiffs and Class members have suffered harm because, among other things, their PII and PHI has been exposed, imminently subjecting each member of the Class to identity theft, credit and bank fraud, social security fraud, tax fraud, medical-identity fraud, and other varieties of identity fraud.

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

106. Banner's actions have substantially increased the risk of Plaintiffs and the Class members to identity theft and medical-identity theft as set forth above.

107. As a direct and proximate result of Banner's actions, Plaintiffs and the Class members require comprehensive and effective credit, identity, and medical-identity monitoring to ensure that they can immediately detect and timely respond to attempts by cyber criminals to steal their credit, identities, and/or medical identities. There exist effective means of monitoring such activities but the credit monitoring offered by Banner is woefully inadequate to do so. Plaintiffs seek damages in this case to provide Plaintiffs and the Class comprehensive and effective credit, identity, and medical-identity monitoring.

COUNT II

(Negligence Per Se; HIPAA, the FTC Act)

108. Plaintiffs incorporate herein the allegations in the previous paragraphs.

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

110. Based on those requirements and in order to obtain services from Banner, Plaintiffs and Class members provided Banner with a massive amount of PII and PHI belonging to Plaintiffs and Class members.

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

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

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

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

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

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

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

118. As a direct and proximate result of Banner's breaches of it duties, Plaintiffs and Class members have suffered harm because, among other things, their PII and PHI has been exposed, imminently subjecting each member of the Class to identity theft, credit and bank fraud, social security fraud, tax fraud, medical identity fraud, and other varieties of identity fraud.

119. Plaintiffs and the Class members have suffered monetary damages and/or will incur monetary damages in the future both in an effort to protect themselves and to remedy acts of fraudulent activity. Plaintiffs and the Class members have suffered,

and/or face an imminent risk of suffering, the theft of their credit identity and medical identities; costs associated with prevention, detection, and mitigation of identity theft, medical identity theft, and/or fraud; costs associated with time spent and productivity loss resulting from addressing the consequences of, or preventing, fraud in any of its forms; and damages from the unconsented exposure of PII and PHI due to this breach.

COUNT III

(Negligence Per Se, A.R.S. § 44-7501(A), 45 CFR § 164.404)

120. Plaintiffs incorporate herein the allegations in the previous paragraphs.

121. Banner owed and owes Plaintiffs and all Class members a duty of reasonable care to notify them in an expedient manner and without unreasonable delay if their PII, PHI, or other sensitive information was potentially exposed to unauthorized access.

122. Under A.R.S. § 44-7501(A), once Banner became aware of the breach, it was required to provide notice to Plaintiffs and all Class members in the "most expedient manner possible and without unreasonable delay."

123. Under 45 CFR § 164.404, as a covered entity, Banner is required to provide notification to each individuals whose PHI has been or is reasonably believed to have been accessed, acquired, used, or disclosed as a result of a breach "without unreasonable delay and in no case later than 60 calendar days after discovery of a breach."

124. Through its acts and omissions, including those described above, Banner violated its obligations under A.R.S. § 44-7501 and its duty of care to provide notification to Plaintiffs and the Class members in the most expedient manner possible and without unreasonable delay. The notice provided by Banner was not done in the most expedient manner possible and was subject to unreasonable delay.

125. As a direct and proximate result of Banner's breach, Plaintiffs and Class members have suffered harm. Banner's unreasonable delay in providing notice left Plaintiffs and the Class members further exposed to identity theft for a significant period

of time. It also denied them the opportunity to take earlier affirmative steps to protect their identities, accounts, and credit from access and theft.

COUNT IV

(Promissory Estoppel)

126. Plaintiffs incorporate herein the allegations in the previous paragraphs.

127. Banner made numerous representations to Plaintiffs and Class members, including but not limited to those set forth in paragraphs 22 through 24 above, that it would protect and maintain the security and confidentiality of their PII and PHI.

128. Banner made these representations for the express purpose of inducing Plaintiffs and Class members to enter into relationships with them for the provision of healthcare services and other services. It was reasonably foreseeable that Plaintiffs and Class members would rely on these promises in part because Banner made so many representations to protect the confidentiality of the information but also because the type of information at issue is almost never disclosed by owners without assurances of protection due to the dramatic harm that can befall them if the information gets in the wrong hands.

129. These representations were material to Plaintiffs and Class members. Plaintiffs and Class members expressly relied on these representations by supplying Banner with their PII and PHI. And, in the absence of such promises and representations to protect their confidential PII and PHI, Plaintiffs and Class members would not have provided their PII and PHI to Banner. Indeed, had Banner not promised to protect their confidential information or disclosed that it would not do so, Plaintiffs and Class members would have sought healthcare services and other services from other providers.

130. As a result of Banner's failure to protect their PII and PHI, Plaintiffs and Class members relied on Banner's promises and representations to their detriment. By virtue of Banner's failure to protect the information and the subsequent breach of its systems by cyber criminals, the PII and PHI of Plaintiffs and the Class members has been stolen, subjecting them to credit theft, identity theft, and medical-identity theft.

Additionally, Plaintiffs and Class members have incurred or will incur direct costs associated with protecting themselves from such criminal activities and restoring harm caused by them.

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

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

133. As a direct and proximate result of Banner's breach of its promises and representations, Plaintiffs and Class members have suffered actual damages resulting from the theft of their PII and PHI and remain at imminent risk of suffering additional damages in the future by credit theft, identity theft, and medical-identity theft.

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

COUNT V

(Negligent Misrepresentation)

135. Plaintiffs incorporate herein the allegations in the previous paragraphs.

136. Banner negligently and recklessly misrepresented material facts pertaining to the sale of healthcare services and other services by representing to Plaintiffs and Class members that it would maintain adequate data privacy and security practices and procedures to safeguard Plaintiffs' and Class members' PII and PHI from unauthorized disclosure, release, data breaches, and cyberattack.

137. Banner negligently and recklessly misrepresented material facts relating to the sale of healthcare services and other services to Plaintiffs and Class members by

representing that it would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of Plaintiffs' and Class members' PII and PHI.

138. Because of the numerous reported incidents of data breaches and public information readily available as to the threats to the particular information Banner had on its information systems, Banner either knew or should have known that its representations were not true.

139. In reliance upon Banner's misrepresentations, Plaintiffs and Class members purchased healthcare services and other services from Banner.

140. Had Plaintiffs 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 Class members' PII and PHI, they would not have purchased healthcare services or other services from Banner, and would not have entrusted their PII and PHI to Banner.

141. As a direct and proximate consequence of Banner's negligent misrepresentations, Plaintiffs and Class members have suffered the injuries alleged above.

COUNT VI

(Unjust Enrichment)

142. Plaintiffs incorporate herein the allegations in the previous paragraphs.

143. In the alternative to the claims alleged above, Plaintiffs allege that they have no adequate remedy at law and bring this unjust enrichment claim on behalf of the Class members.

144. Plaintiffs and Class members conferred a monetary benefit on Banner in the form of payments for healthcare services and other services. Plaintiffs and Class members also provided their PII and PHI to Banner.

145. Banner appreciated or had knowledge of the benefits conferred by Plaintiffs and Class members.

146. The payments for healthcare services and other services that Plaintiffs and Class members paid, directly or indirectly, to Banner should have been used by Banner, in part, to pay for the administrative costs of reasonable data privacy and security practices and procedures.

147. As a result of Banner's conduct described herein, Plaintiffs and Class members suffered actual damages in an amount equal to the difference in value between healthcare and other services associated with the reasonable data privacy and security practices and procedures for which Plaintiffs and Class members, and the inadequate healthcare services and other services without reasonable data privacy and security practices and procedures that they received.

148. Under principles of equity and good conscience, Banner should not be permitted to retain money belonging to Plaintiffs and Class members because Banner failed to use that money to implement the reasonable data privacy and security practices and procedures for which Plaintiffs and Class members paid and that were otherwise mandated by HIPAA regulations, federal and state law, industry standards, and best practices.

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

150. A constructive trust should be imposed upon all unlawful or inequitable sums received by Banner traceable to Plaintiffs and Class members.

COUNT VII

(Breach of Fiduciary Duty)

151. Plaintiffs incorporate herein the allegations in the previous paragraphs.

152. As a healthcare provider to Plaintiffs and the Class members, Banner occupied a position of special trust and has special duties with respect to its dealings with Plaintiffs and the Class. Specifically, as a healthcare provider, Banner has special obligations to Plaintiffs and the Class with respect to their personal healthcare and medical information. Such information is protected from disclosure by law in every state

as privileged, and Banner has affirmative obligations to Plaintiffs and Class members to protect it from dissemination and disclosure by state and federal statutes and common law.

153. By requiring Plaintiffs and the Class members to provide confidential PII and PHI to Banner, Banner took on a fiduciary obligation to Plaintiffs and the Class members to secure their PII and PHI and to protect it from unauthorized access and disclosure. Banner obtained and stored the PII and PHI by inviting the trust of Plaintiffs and the Class members, and Plaintiffs and the Class members reposed their trust in Banner to secure and protect their PII and PHI.

154. In reliance on Banner's special duties and obligations to protect their PII and PHI from disclosure and the fiduciary relationship with Banner with respect to that information, Plaintiffs and the Class members entrusted Banner with their PII and PHI.

155. Through its acts and omissions, including those described above, Banner breached its fiduciary duty to Plaintiffs and the Class members.

156. As a direct and proximate result of Banner's breach, Plaintiffs and Class members have suffered harm.

COUNT VIII

(Breach of the Right of Privacy)

157. Plaintiffs incorporate herein the allegations in the previous paragraphs.

158. Plaintiffs and the Class members have a legally protected privacy interest in their PII and PHI that existed and was maintained on Banner's electronic information systems. The combination of information that comprises the PII and PHI of each Plaintiff and each Class member is private information. When combined, a person's name, date of birth, address, and social security number provide sufficient information for even relatively unsophisticated identity thieves to use a person's personal information to commit identity theft, credit fraud, or to access the person's financial accounts. Consequently, people (including Plaintiffs and the Class members) treat such information

as private facts. Additionally, the PHI of Plaintiffs and Class members is some of the most personal, private, and otherwise protected information any individual owns.

159. The PII and PHI of Plaintiffs and Class members is information that disclosure of which to the public would be highly offensive to a reasonable person in that such disclosure would subject them to identity theft and credit theft.

160. Plaintiffs and the Class members had a reasonable expectation that the PII and PHI that they entrusted to Banner would remain private and not subject to disclosure to, or to access by, unauthorized persons. In particular, Plaintiffs and the Class members had a reasonable expectation that Banner would take reasonable efforts to ensure that their private PII and PHI could not be accessed, viewed, or acquired by anyone other than authorized persons within Banner.

161. The private PII and PHI of Plaintiffs and the Class members is not of legitimate concern to the public and its exposure to the public would be highly offensive to a reasonable person. Indeed, private PII and PHI, like the private PII and PHI of Plaintiffs and the Class, is guarded by most members of the public precisely because that information is not of legitimate concern to the public and its exposure could have adverse effects. Additionally, the PHI of Plaintiffs is personal, protected, and privileged information under Arizona law and the law of every state. As such, its disclosure to third parties would be highly offensive to a reasonable person.

162. Through its acts and omissions, including those described above, Banner violated the rights of privacy of Plaintiffs and the Class members. As a direct and proximate result, Plaintiffs and the Class members have suffered harm and will continue to suffer harm, including but not limited to the ongoing exposure of their PII and PHI by virtue of Banner's failure to correct the problems that resulted in the Banner breach.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and the Class, pray for judgment in their favor and against Banner as follows:

A. For an order certifying this matter as a class action lawsuit under Rule 23, Fed. R. Civ. P, to proceed on behalf of the Class, appointing Plaintiffs and their counsel to represent the Class, and directing that reasonable notice be given by Banner to all Class members;

B. For such compensatory damages as proven at trial or otherwise;

C. For injunctive relief requiring that Banner (a) provide reasonable and adequate notice to all affected individuals in accordance with A.R.S. § 44-7501(A), (b) take all necessary steps to ensure that the PII and PHI of Plaintiffs and the Class members is secure and cannot be accessed, viewed, or acquired unless authorized by law, (c) provide lifetime comprehensive credit-monitoring and identity-theft-repair services for Plaintiffs and Class members, (d) establish a fund to compensate Plaintiffs and Class members for costs associated with protecting their medical identity and preventing its theft, and (e) establish a fund to compensate those Class members who suffer identity or medical-identity theft due to their PII and PHI being exposed by this breach;

D. For an award of all costs and expenses incurred in this action; and

E. For such other and further relief as the Court deems appropriate.

DEMAND FOR JURY TRIAL

Plaintiffs demand trial by jury of all issues so triable.

RESPECTFULLY submitted this 23rd day of August 2016.

GALLAGHER & KENNEDY, P.A.

By: */s/ Paul L. Stoller*

Paul L. Stoller
C. Lincoln Combs
2575 East Camelback Road
Phoenix, Arizona 85016-9225

Hadley L. Matarazzo (*pro hac* forthcoming)
Kathryn Bruns (*pro hac* forthcoming)
FARACI LANGE, LLP
28 East Main Street, Suite 1100
Rochester, New York 14614
Telephone: (585) 325-5150
Email: hmatarazzo@faraci.com

Counsel for Plaintiffs and the Putative Class

5582153/27653-0001