HAGENS BERMAN SOBOL SHAPIRO LLP
Robert B. Carey (011186)
Leonard W. Aragon (020977)
Michella A. Kras (022324)
11 West Jefferson Street, Suite 1000
Phoenix, Arizona 85003
Telephone: (602) 840-5900
Facsimile No.: (602) 840-3012
E-Mail: rob@hbsslaw.com
leonard@hbsslaw.com
michellak@hbsslaw.com

Counsel for Plaintiff

THE SUPERIOR COURT OF THE STATE OF ARIZONA

IN AND FOR THE COUNTY OF MARICOPA

Howard Chen, individually and on behalf of all other similarly situated,

Plaintiff,

vs.

Banner Health,

Defendant.

No. CV 2016-011988

CLASS ACTION COMPLAINT
(Jury Trial Requested)

Plaintiff, Dr. Howard Chen, individually and as a class representative on behalf of all similarly situated persons and the general public, brings this class action complaint against Banner Health ("Banner Health") and allege as follows:

I. INTRODUCTION

1. A health system that requests and then retains millions of individuals' personally identifiable information must ensure that the information is safeguarded from theft. This lawsuit stems from Banner's failure to secure the data of its patients,

employees, plan members and beneficiaries, customers at food and beverage outlets, and providers.

2. Banner is a health system based in Phoenix Arizona.

3. Banner operates 31 hospitals and medical centers in Arizona, Alaska, California, Colorado, Nebraska, Nevada, and Wyoming, in addition to operating hundreds of health clinics. Banner employs over 39,000 employees in Arizona. In 2010, Banner reported assets of $6.4 billion and revenues of $4.9 billion.

4. In late June, 2016, Banner discovered that hackers accessed multiple Banner databases, including payment-card records for Banner's food and beverage services and patient and health insurance records. Upon information and belief, the breach affects 3.7 million patients, health-insurance customers, cafeteria customers, doctors, and other health-care providers.

5. As a result of the Banner data breach, the names, addresses, phone numbers, email addresses, Social Security Numbers, dates of birth, financial and bank account information, and medical information, including doctors' names, dates of service, claims information, and health-insurance information, have been exposed to fraud and these individuals have been harmed as a result. The harm to victims of the Banner data breach includes expenses related to credit monitoring, credit restoration, and identity theft prevention, and the time and inconvenience of dealing with issues resulting from the unauthorized disclosure of personal information. Plaintiff seeks to remedy these harms, and prevent their future occurrence, on his behalf and on behalf of all victims of the Banner data breach.

II. PARTIES, JURISDICTION AND VENUE

6. Plaintiff Howard Chen is a resident of Maricopa County, Arizona.

7. Banner Health is a health services provider with its principal place of business in Maricopa County, Arizona.

8. This court has jurisdiction pursuant to A.R.S. § 12-123.

9. Venue is proper in this court pursuant to A.R.S. § 12-401.

10. Upon information and belief more than two-thirds of all putative class members reside in Arizona.

11. Upon information and belief, executive decisions relating to the collection, retention, security, and dissemination of personally identifiable information health information, credit card information, and provider information of putative class members took place in Maricopa County, Arizona.

12. Upon information and belief, all or most electronically stored personally identifiable information, health information, credit card information, and provider information of putative class members is retained and "secured" in Arizona.

13. Upon information and belief, all or most relevant Banner Health data security team members and information technology staff are located in Arizona, and all relevant decisions related to data security were made in Arizona.

14. Upon information and belief, the principal injuries, including the collection and retention of putative class members' personally identifiable information, health information, credit card information, and provider information took place in Maricopa County, Arizona.

15. Upon information and belief, no class action asserting similar factual allegations has been filed against Banner in the preceding three years.

III. FACTS

A. Banner Health Collects and Stores Personal and Financial Information for its Patients, Employees, Providers and Customers.

16. Banner collects and maintains information on patients, employees, health professionals, and cafeteria and health-insurance customers.

17. Banner collects and maintains personal information about its patients, employees, and health-insurance customers, including names, addresses, Social Security Numbers, birth dates, doctors' information, insurance information, and claims information.

18. Additionally, Banner collects and maintains payment information of its customers, including cardholder name, card number, expiration date and internal verification codes.

19. Banner also collects and maintains provider information, including names, addresses, birthdates, Social Security Numbers, Taxpayer Identification Numbers, Drug Enforcement Agency numbers, and National Provider Identifier numbers.

B. Banner's Data Breach.

20. On June 29, 2016 Banner's information technology staff detected unlawful activity on Banner's servers.

21. With the assistance of an outside cyber security firm, Mandiant, Banner reported that hackers may have accessed Banner's computer system that processes payment card data at the food and beverage outlets at several Banner locations in Alaska, Arizona, Colorado and Wyoming.

22. Upon information and belief, hackers did access Banner's computer systems that process payment card data.

23. The hackers targeted transactions that took place between June 23 and July 7, 2016.

24. On July 13, 2016 Banner detected that hackers also may have accessed patient and health insurance records, which includes names, birth dates, addresses, doctors' names, dates of service, claims information, health-insurance information and Social Security numbers.

25. Upon information and belief, hackers did access patient and health records.

26. Many of Banner's employees and health professionals were also enrolled in Banner's health insurance and were patients of Banner.

27. On August 3, 3016, Banner sent emails to its employees informing them of the data breach.

28. In that email Banner stated "[i]t is possible that information of approximately 3.7 million individuals may be affected by this incident."

29. The email further states: "This information may include name, birthdate, Social Security number, address, physician names, dates of service, clinical information, and possibly health insurance information if you are a member of a health plan we administer."

30. Additionally, according to Banner, "[e]mployed and community providers' affected information may include, name, address, birthdate, Social Security number, Taxpayer Identification Number (TIN), Drug Enforcement Agency (DEA) number, and National Provider Identifier (NPI) number,"

31. Banner told employees it was starting the process of sending letters to all affected individuals to inform them of the breach and offer one year of credit and identity monitoring from Kroll.

32. Banner represented in its email that it "is committed to maintaining the privacy and security of information of our patients, employees, plan members and beneficiaries, customers at our food and beverage outlets, as well as our providers."

C. Plaintiff's Personal Information Is at Risk Because of the Security Breach.

33. Dr. Howard Chen is currently hospital staff at Banner Thunderbird hospital.

34. From 2010 to 2013 Dr. Chen was employed by Banner Arizona Medical Clinic (now Banner Medical Group).

35. While employed at Banner, Dr. Chen was enrolled in Banner Health Insurance.

36. Upon information and belief, Dr. Chen's personal information was compromised in three different ways: as an employee, insurance customer, and health provider.

37. Dr. Chen is concerned that as a result of Banner's conduct, his personal information, provider information, and health information is vulnerable to use by third parties.

38. As a result of the data breach, Dr. Chen will be forced take affirmative measures, including personal financial outlays and time away from his medical practice, to ensure that his personally identifiable information, health information, and provider information is protected.

D. The Data Breach Harmed Plaintiff and Other Class Members.

39. Banner's offer of a single year of credit monitoring fails to address the damage caused by the breach.

40. Cyber criminals would not have access to Banner's databases but for Banner's inadequate security protections, particularly given the type of sensitive and valuable information Banner maintained.

41. The basic levels of services offered by Banner through Kroll are insufficient to protect Class members from data breached.

42. As a result of Banner's inadequate and unreasonable data security, cyber-criminals may have the ability to sell or use the personal information of Plaintiff and the Class and, in the case of customers, their financial information as well. As a result, breach victims must add themselves to credit fraud watch lists, which substantially impair the victims' ability to obtain additional credit. Because names, addresses, birthdates and Social Security numbers were stolen, there is a real and compounding risk that Plaintiff and the Class will be victims of identity theft.

43. Personal and financial information is a valuable commodity. A "cyber black-market" exists in which criminals openly post stolen credit card numbers, Social Security numbers, and other personal information on a number of Internet websites.

44. The personal information that Banner failed to adequately protect, including Plaintiff's identifying information, is "as good as gold" to identity thieves

because identity thieves can use victims' personal data to open new financial accounts and incur charges in another person's name, take out loans in another person's name, incur charges on existing accounts, or clone ATM, debit, or credit cards.

45. As reported by the Identity Theft Protection Association, "[T]he ongoing exposure of confidential consumer and business information through data security breaches fuels a thriving internet black market in which this sensitive information is traded, sold, and re-sold on a daily basis through online black market websites, secret chat rooms, and underground forums."[1]

46. According to the Office of the National Counterintelligence Executive, the cost to purchase an individual's personal information is surprisingly low, sometimes as little as a few dollars, making it highly likely that Plaintiff's and Class members' PII is available for sale or has already been sold on the black market.[2]

47. Plaintiff and the Class are also in danger of having medical identity theft and health insurance fraud.

48. According to Bob Gregg, chief executive of ID Experts in Portland, Oregon, detailed medical records are often more valuable than credit card information, addresses or Social Security numbers, because medical records have unique identifiers, which can result in medical-identity theft and fraudulent health insurance or prescription drug bills.[3]

49. Mr. Gregg further explained that detailed medical records with unique patient identifying numbers can cost as much as $100 per record.[4]

---

[1] Barnett, Michael. The Internet Information Black Market, *available at* http://businessidtheft.org/Education/BusinessIDTheftScams/InternetBlackMarket/tabid/117/Default.aspx

[2] *See* Office of the National Counterintelligence Executive, How Much Do You Cost On The Black Market, *available at* http://www.ncix.gov/issues/cyber/identity_theft.php.

[3] Ken Alltucker, Banner Health Cyberattack Breaches up to 3.7 Million Records, available at http://www.azcentral.com/story/money/business/health/2016/08/03/banner-health-cyberattack-breaches-up-3-7-million-records/88035474/

[4] *Id.*

E. Banner's Offer of a Single Year of Credit Monitoring Is Inadequate.

50. Although Banner is offering free credit monitoring, the credit monitoring services will not prevent identity theft or protect Plaintiff and the Class for more than a year. It also will not protect their health or provider information. Meanwhile all of this information could be misused by identity thieves and others years into the future.

51. Moreover, experts warn that when a breach occurs "[o]ne year of credit monitoring may not be enough. Hackers tend to lay low when data breaches are exposed…They often wait until consumers are less likely to be on the lookout for fraudulent activities."[5] Thus, Plaintiff and the Class must take additional steps to protect their credit and identities.

52. Plaintiff and the Class members' health information and personally identifiable information is also valuable to identity thieves because identity thieves can use it to commit insurance fraud, medical identity theft, open new financial accounts, access existing accounts, take out loans and incur charges in Plaintiff's and Class members' names, and clone ATM, debit or credit cards.

53. In fact, the FTC recommends placing an extended fraud alert with each credit reporting agency after your identity has been compromised.[6] These fraud alerts last for seven years.

54. The FTC also recommends taking multiple steps once your data has been compromised, which depending upon the circumstances may include: placing a fraud alert, requesting a credit freeze, ordering your credit reports, creating an identity theft report, and filing a police report.

55. And, according to a 2011 report by Javelin Strategy and Research, individuals who receive a data breach notification letter are more than four times as likely

---

[5] Available at http://online.wsj.com/news/articles/SB10001424052702304856504579337263720948556

[6] Available at https://www.consumer.ftc.gov/articles/pdf-0009-taking-charge.pdf

to become victims of identity theft, average out-of-pocket costs to remedy a data breach are $631, and data breach victims spend an average of 41 hours resolving the breach.[7]

56. While Banner has reported that it notified the Arizona Medical Board and Drug Enforcement Administration regarding the compromised provider and DEA numbers, Kroll's free credit monitoring does not cover this data. Thus, physicians and providers will have to continually monitor for misuse of this data.

IV. CLASS ALLEGATIONS

57. Under Rule 23 of the Arizona Rules of Civil Procedure, Plaintiff brings this action as a class action for himself and all members of the following Class of similarly situated individuals and entities:

> All persons whose personally identifiable information, health information, credit card information, or health provider information was stored on Banner's electronic data systems at any time between June 23, 2016 to August 3, 2016[8] and all persons who engaged in a credit transaction at any Banner food and beverage outlet identified by Banner Health as being compromised between June 23, 2016 and July 7, 2016.

58. Excluded from the Class are Banner, its co-conspirators, officers, directors, legal representatives, heirs, successors and wholly or partly owned subsidiaries or affiliated companies; class counsel and their employees; and the judicial officers and their immediate family members and associated court staff assigned to this case, and all persons within the third degree of relationship to any such persons.

59. ***Numerosity***. The Class is so numerous that joinder of all members is unfeasible and not practical. While the precise number of Class members has not been determined at this time, 3.7 million persons either had their personally identifiable

---

[7] Javelin Strategy & Research, "2011 Identity Fraud Survey Report," February 2011, available at https://www.javelinstrategy.com/uploads/1103.R_2011%20Identity%20Fraud%20Survey%20Consumer%20Report.pdf.

[8] Plaintiff reserves the right to amend the class definition after discovery.

information, credit card information, heath information, or health provider information compromised in the data breach that Banner first disclosed on August 3, 2016.

60. ***Commonality***. Questions of law and fact common to all Class members exist and predominate over any questions affecting only individual Class members, including, *inter alia*:

a. whether Banner implemented reasonable and industry-standard safety measures to protect Class members' personally identifiable information, credit card information, heath information, or health provider information;

b. whether Banner knew or should have known that its information technology systems were not secure;

c. whether Banner was negligent in adopting, designing, implementing, or supervising its information technology security systems;

d. whether Plaintiff and Class members are entitled to recover compensatory damages, including credit monitoring, and/or other equitable relief.

61. ***Typicality***. Plaintiff's claims are typical of the claims of the Class. Plaintiff and all Class members were injured through the uniform misconduct described above and assert the same claims for relief, all of which arose out of the same scheme or conduct. While not all aspects of each Class members' circumstances are identical, the material aspects of their claims are typical.

62. ***Adequacy***. Plaintiff and his counsel will fairly and adequately represent the interests of the Class members. Plaintiff has no interests antagonistic to, or in conflict with, the interests of the other Class members, and he will zealously pursue the claims in this action. Plaintiff's lawyers are highly experienced in the prosecution of consumer class actions and complex commercial litigation, capable of providing the financial resources necessary to litigate this matter to conclusion, and have litigated other data breach matters in a class context.

63. ***Superiority***. A class action is superior to all other available methods for fairly and efficiently adjudicating the claims of Plaintiff and the Class members. Plaintiff

and the Class members have been harmed by Banner's wrongful actions and/or inaction. Litigating this case as a class action will reduce the possibility of repetitious litigation relating to Banner's wrongful actions and/or inaction, and provides an efficient mechanism for adjudication for Class members, most of whose claims are too small to warrant individual litigation.

64. Class certification is appropriate under Ariz. R. Civ. P. 23(b)(3), because the above common questions of law or fact predominate over any questions affecting individual members of the Class, and a class action is superior to other available methods for the fair and efficient adjudication of this controversy.

65. As to claims for injunctive or declaratory relief, class certification is appropriate under Ariz. R. Civ. P. 23(b)(2) because Banner has acted or refused to act on grounds generally applicable to the Class, so that final injunctive relief or corresponding declaratory relief is appropriate as to the Class as a whole.

66. Class certification is appropriate under Ariz. R. Civ. P. 23(b)(1), because prosecuting separate actions by individual class members would create a risk of inconsistent or varying adjudications with respect to individual members of the class which would establish incompatible standards of conduct for the party opposing the class, or adjudications with respect to individual members of the class which would as a practical matter be dispositive of the interests of the other members not parties to the adjudications or substantially impair or impede their ability to protect their interests.

67. The expense and burden of litigation would substantially impair the ability of Plaintiff and Class members to pursue individual lawsuits to vindicate their rights on an efficient basis. Absent a class action, Banner will have wrongfully jeopardized the personal information, credit card information, heath information, or health provider information of Class Members and shifted the risk of problems and misuse to the Class Members. Through the use of effective, long-term credit monitoring and identity protection services, the deleterious effects of Banner's misconduct can be mitigated or prevented.

V. CLAIMS FOR RELIEF

CLAIM I

Negligence

68. Plaintiff realleges and incorporates by reference the allegations contained in the preceding paragraphs.

69. By requesting and accepting Plaintiff's and Class members' personally identifiable information, credit card information, heath information, or health provider information, Banner assumed a duty requiring it to use reasonable and industry standard care to secure such information against theft and misuse.

70. Banner breached its duty of care by failing to adequately secure and protect Plaintiff's and the Class members' personally identifiable information, credit card information, heath information, or health provider information from theft, collection, and misuse by third parties.

71. Among other things, Banner's failure to safeguard Plaintiff's and Class members' personally identifiable information, credit card information, heath information, or health provider information and the resulting data breach, has left Plaintiff and Class members exposed to greatly increased, long-term risk of identity theft and medical-identity theft, including without limitation well-known risks of credit damage, reputational harm, insurance fraud, and financial loss.

72. Routine and robust credit monitoring and identity protection is necessary to protect Class members, to the extent possible, from credit damage, reputational harm, and financial loss.

73. Plaintiff and the Class have suffered injury in fact, and will continue to be injured and incur damages as a result of Banner's negligence and misconduct.

74. As a direct and proximate result of Banner's failure to take reasonable care and use industry standard measures to protect the personally identifiable information, credit card information, heath information, or health provider information placed in its

care, Plaintiff's and Class members' personally identifiable information was disclosed or acquired by unauthorized parties, to the detriment of each Class member.

75. As a direct and proximate result of Banner's negligence and misconduct, Plaintiff and the Class were injured in fact by the unauthorized disclosure of their personally identifiable information, credit card information, heath information, or health provider information and are entitled to recover the costs associated with the detection and prevention of identity theft and medical-identity theft, including credit monitoring, identity theft consultation, and identity restoration, and with the detection and prevention of unauthorized use of their financial accounts, including credit monitoring, all of which have an ascertainable monetary value to be proven at trial.

CLAIM II

Breach of Contract

76. Plaintiff realleges and incorporates by reference the allegations contained in the preceding paragraphs.

77. As a condition of employment, receiving treatment, acting as a medical provider, or as a health insurance or food service customer, Banner requested Plaintiff's and Class members' personally identifiable information, credit card information, heath information, or health provider information. Plaintiff and Class members provided that information to Banner in accordance with Banner's contractual requirements.

78. Banner had a contractual duty to maintain and safeguard that information.

79. Banner breached its contractual duties when it failed to protect Plaintiff's and the Class members' personally identifiable information, credit card information, heath information, or health provider information.

80. Among other things, Banner's failure to safeguard Plaintiff's and Class members' personally identifiable information, credit card information, heath information, or health provider information and the resulting data breach, has left Plaintiff and Class members exposed to greatly increased risk of identity theft, medical-identity theft,

including without limitation well-known risks of credit damage, insurance fraud, reputational harm, and financial loss.

81. Routine and robust credit monitoring and identity protection is necessary to protect Class members, to the extent possible, from credit damage, reputational harm, insurance fraud, and financial loss.

82. Plaintiff and the Class have suffered injury in fact, including monetary damages, and will continue to be injured and incur damages as a result of Banner's breach of contract.

83. As a natural and probable consequence of Banner's breach of contract, Plaintiff's and Class members' personally identifiable information credit card information, heath information, or health provider information was disclosed to unauthorized parties, to the detriment of each Class member.

84. Because of Banner's breach of contract, Plaintiff and the Class were injured in fact by the unauthorized disclosure of their personally identifiable information, credit card information, heath information, or health provider information and are entitled to recover all costs associated with the detection and prevention of identity theft, including credit monitoring, identity theft consultation, and identity restoration, and with the detection and prevention of unauthorized use of their financial accounts, all of which have an ascertainable monetary value to be proven at trial.

CLAIM III

Invasion of Privacy

85. Plaintiff realleges and incorporates by reference the allegations contained in the preceding paragraphs.

86. Arizona law protects an individual's right to privacy.

87. Article II § 8 of the Arizona Constitution guarantees that "[n]o person shall be disturbed in his private affairs, or his home invaded, without authority of law."

88. Public disclosure of private facts is one form of invasion of privacy.

89. The data breach, which resulted in the theft of Banner's databases on the internet, constitutes public disclosure.

90. Plaintiff's and Class members' personally identifiable information, credit card information, heath information, or health provider information constitutes a private fact.

91. The disclosure of this information is offensive to a reasonable person.

92. The personally identifiable information, credit card information, heath information, or health provider information disclosed is not of legitimate public concern.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff respectfully requests the following relief:

A. That the Court certify this case as a class action and appoint Plaintiff Dr. Howard Chen to be class representative and Hagens Berman Sobol Shapiro LLP, as class counsel;

B. That the Court certify Plaintiff's claims under Ariz. R. Civ. P. 23(b)(3) and/or Ariz. R. Civ. P. 23(b)(2) and/or 23(b)(1);

C. That the Court award Plaintiff appropriate compensatory damages, including without limitation damages associated with credit monitoring, credit restoration, and identity protection, as well as any and all monies that should have been incurred by Defendant to protect Class members' personally identifiable information, credit card information, heath information, or health provider information;

D. Any declaratory or injunctive relief sought or required to effect justice;

E. An award of attorneys' fees to Class Counsel and an incentive award for Plaintiff, each in an amount deemed reasonable by this Court; and

F. That the Court award Plaintiff such other, relief as may be available and appropriate.

DATED this 5th day of August, 2016.

Respectfully submitted,

HAGENS BERMAN SOBOL SHAPIRO LLP

By _____

Robert B. Carey
Leonard W. Aragon
Michella A. Kras
11 West Jefferson Street, Suite 1000
Phoenix, Arizona 85003
Telephone: (602) 840-5900
Facsimile No.: (602) 840-3012
E-mail: rob@hbsslaw.com
leonard@hbsslaw.com
michellak@hbsslaw.com

HAGENS BERMAN SOBOL SHAPIRO LLP
Robert B. Carey (011186)
Leonard W. Aragon (020977)
Michella A. Kras (022324)
11 West Jefferson Street, Suite 1000
Phoenix, Arizona 85003
Telephone: (602) 840-5900
Facsimile No.: (602) 840-3012
E-Mail: rob@hbsslaw.com
leonard@hbsslaw.com
michellak@hbsslaw.com

Counsel for Plaintiff

THE SUPERIOR COURT OF THE STATE OF ARIZONA

IN AND FOR THE COUNTY OF MARICOPA

Howie Chen, individually and on behalf of all other similarly situated,

Plaintiffs,

vs.

Banner Health,

Defendant.

No: CV 2016-011988

DEMAND FOR JURY TRIAL

Pursuant to Ariz. R. Civ. P. 38(b), Plaintiff Howie Chen hereby requests a trial by jury of all issues triable of right by a jury in the above-entitled action.

DATED this 5th day of August, 2016.

Respectfully submitted,

HAGENS BERMAN SOBOL SHAPIRO LLP

By _____

Robert B. Carey
Leonard W. Aragon
Michella A. Kras
11 West Jefferson Street, Suite 1000
Phoenix, Arizona 85003
Telephone: (602) 840-5900
Facsimile: (602) 840-3012
E-mail: rob@hbsslaw.com
leonard@hbsslaw.com
michellak@hbsslaw.com

Attorneys for Plaintiff