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: (602) 840-3012
rob@hbsslaw.com
leonard@hbsslaw.com
michellak@hbsslaw.com

BONNETT, FAIRBOURN, FRIEDMAN & BALINT, P.C.
Elaine A. Ryan (012870)
Carrie A. Laliberte (032556)
2325 E. Camelback Road, Suite 300
Phoenix, Arizona 85016
Telephone: (602) 274-1100
eryan@bffb.com
claliberte@bffb.com

BONNETT, FAIRBOURN, FRIEDMAN & BALINT, P.C.
Patricia N. Syverson (AZ Bar No. 020191)
Manfred M. Muecke (*To be admitted Pro Hac Vice*)
600 W. Broadway, Suite 900
San Diego, California 92101
Telephone: (619) 798-4593
psyverson@bffb.com
mmuecke@bffb.com

Counsel for Plaintiffs and the Proposed Class
[Additional attorneys on signature page]

THE SUPERIOR COURT OF THE STATE OF ARIZONA

IN AND FOR THE COUNTY OF MARICOPA

In re: Valley Anesthesiology Consultants, Inc. Data Breach Litigation This Document Relates to: *Becher et al v. Valley Anesthesiology Consultants, Inc.* Case No. CV2016-013446 *Manz et al v. Valley Anesthesiology Consultants, Inc.* Case No. CV2016-052906	Case No. CV2016-013446 FIRST AMENDED CONSOLIDATED CLASS ACTION COMPLAINT FOR: 1. Negligence; 2. Violation of the Arizona Consumer Fraud Act, A.R.S. §§44-1521, *et seq.*; 3. Breach of Express Contract; and 4. Breach of Implied Contract. [JURY TRIAL DEMANDED] (Assigned to the Hon. Daniel Martin)

Plaintiffs Cade Becher, Melanie R. Chaignot, Janice E. Manz, and Megan F. Thomas, individually and as class representatives on behalf of all similarly situated persons, bring this class action complaint against Valley Anesthesiology Consultants, Inc., formerly Valley Anesthesiology Consultants, Ltd., d/b/a Valley Anesthesiology and Pain Consultants ("VAPC") and allege as follows:

NATURE OF THE ACTION

1. Plaintiffs and Class Members are consumers of medical care and services, current and former employees, and current and former health-care providers who all entrusted their personally identifiable information ("PII"), payment card industry ("PCI") and medical records and private health information ("PHI") to VAPC.

2. VAPC is a group of 300 anesthesiology and interventional pain management providers based in Phoenix, Arizona.

3. VAPC provides services at twenty-five facilities across the Valley of the Sun, including Valley Anesthesiology Health, Barrow Neurological Institute, Phoenix Children's Hospital, Scottsdale Healthcare System, and St. Joseph's Hospital.

4. In the course of its business, VAPC demands and retains as a condition of care, employment, and provider privileges hundreds of thousands of individuals' PII, PCI, and PHI. In doing so, VAPC has a duty to ensure the sensitive information it requests, requires and retains is properly safeguarded. VAPC was entrusted with and obligated to safeguard and protect Plaintiffs' and Class Members' PII, PCI, and PHI in accordance with all applicable laws.

5. Despite its obligations to protect the client, employee, and provider PII, PCI, and PHI it demands, collects, and retains, VAPC did not have adequate security systems, protocols, personnel, policies, or infrastructure in place to protect class members' PII, PCI, and PHI.

6. On June 13, 2016, VAPC discovered that several of its computer systems suffered a cyber-attack [redacted] on March 30, 2016, including systems that

contained personal patient information, including medical and insurance records, that were accessible during the unauthorized connections to the VAPC computer systems.

[redacted]

8. According to VAPC, the March 30, 2016 breach affected over 882,000 patients, current and former employees, and health-care providers.

[redacted]

12. Plaintiffs' and Class Members' sensitive PII, PCI, and PHI was, upon information and belief, accessed, acquired, used and/or exfiltrated over a period of several months.

13. On August 12, 2016 – over four and a half months after the initial attack occurred and two months after first learning of the attack – VAPC issued a public announcement notifying affected individuals of the attack and potential security issues regarding their PII, PCI, and PHI. *See* August 12, 2016 Press Release, available at http://www.prnewswire.com/news-releases/valley-anesthesiology-and-pain-consultants-identifies-and-addresses-information-security-incident-300312986.html (last visited March 31, 2017).

14. According to VAPC's August 12 Press Release, "The computer systems may contain patient information, such as patient names, their providers' names, dates of service, places of treatment, names of health insurers, insurance identification numbers, diagnosis and treatment codes, and in some instances, social security numbers. For providers, the computer systems included credentialing information, such as names, dates of birth, social security numbers, professional license numbers, Drug Enforcement Agency (DEA) numbers, National Provider Identifiers (NPIs), as well as bank account information and potentially other financial information. For employees, the computer systems included names, dates of birth, addresses, social security numbers, bank account information and financial information, such as tax information." *Id.*

15. VAPC's press release downplayed the significance of the attack and likelihood that Plaintiffs' and Class Members' data may be used for fraudulent purposes. For example, VAPC failed to provide detailed information to the victims as to the actual extent of this compromise, [redacted]

16. VAPC also informed Class Members that there was "no evidence that any of the information has been accessed or used inappropriately," [redacted]

17. As part of its August 12, 2016 Press Release, VAPC also announced it was mailing letters to the "approximately 882,590 patients, and all current and former employees and providers who may have been affected." *Id*. The form letters that were mailed to affected individuals provided the same basic information as the August 12, 2016 Press Release. *See, e.g.,* Exhibit A (Letter to Cade Becher).

[redacted]

21. VAPC offered only a portion of the putative Class credit monitoring. Other Class Members were offered no protection or safeguards against unknown, future misuse of their information even though VAPC, by its own admission, cannot rule out that their PII, PCI and PHI was accessed, acquired and/or exfiltrated. And, upon information and belief, Class Members have complained to VAPC that only some individuals were offered credit monitoring services. [redacted] Through no fault of their own, Plaintiffs and Class Members are concerned about their identities, finances, medical records, credit, and PII/PCI/PHI, and must regularly and diligently monitor their financial accounts PII, PCI, and PHI.

22. And even if certain Class Members were offered credit monitoring, the services they were offered are insufficient to protect their identities, finances, medical records, credit, and PII/PCI/PHI from future misuse.

23. VAPC knew it was storing valuable, vulnerable, and sensitive information on its servers that were obvious targets for cyber attackers. The data collected and stored by healthcare providers, like VAPC, is among the most sensitive and harmful if misused because it contains highly confidential PII, PCI, and PHI that can lead to false medical claims and changes to one's history, creating diagnosis errors of serious magnitude, and may remain available for such illegal and serious misuse for years.[1] It is so sensitive and personal in nature, and the potential consequences of its unauthorized disclosure so severe, that in 1996 Congress enacted the Health Insurance Portability and Accountability Act ("HIPAA"), requiring the Secretary of the U.S. Department of Health and Human Services ("HHS") to develop regulations protecting the privacy and security of such information, which were subsequently promulgated at Pub. L. 104-191.

[redacted]

25. VAPC's wrongful actions, inaction, and/or omissions resulted in VAPC breaching its duty to protect and safeguard Class Members' personal, health, and financial information, to timely provide full and accurate disclosure regarding any data breach, and to take reasonable steps to contain and minimize any damage caused in the event of such information being compromised.

---

[1] According to a GAO Report, "stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years." *See* U.S. Gov't Accountability Off., GAO-07-737, *Personal Information: Data Breaches Are Frequent, But Evidence of Resulting Identity Theft is Limited; However, the Full Extent Is Unknown,* at 29 (2007), http://www.gao.gov/new.items/d07737.pdf (last visited September 2, 2016).

26. Plaintiffs' and Class Members' concern is reasonable and justified. [redacted] there is an immediate and substantial risk of identity theft, identity fraud, medical fraud, lost medical identities and records, fraudulent credit card activity and opening or re-opening of credit card accounts, phishing, increased mailers marketing products and services including, medical products, medical services, and prescription drugs specifically targeted to their medical conditions.[2] In fact, upon information and belief, Plaintiff Becher and other Class Members have already suffered adverse actions [redacted] such as fraudulent attempts (some of them successful) to access bank accounts, fraudulent credit card charges, and out-of-pocket expenses.

27. Plaintiffs, and upon information and belief other Class Members, have devoted time, effort and monies to ensure their own personal and financial security [redacted] And, upon information and belief, Class Members have complained to VAPC about these efforts and out-of-pocket expenses and requested that VAPC reimburse them. It is unreasonable for Plaintiffs and Class Members to wait for actual misuse – a fraudulent charge on a credit card for example – before taking steps to safeguard their assets, particularly since VAPC offered credit monitoring to some Class Members thereby acknowledging the concreteness of the threat.

28. Plaintiffs bring this action individually and on behalf of all others similarly situated whose personal information, including names, birthdates, Social Security numbers, financial and tax information, medical information (physician names, dates of service, clinical information, insurance information, etc.), and/or physician or provider credentials (Drug Enforcement Agency

---

[2] "Phishing" is an attempt to acquire information (and sometimes, indirectly, money), such as usernames, passwords, and credit card details by masquerading as a trustworthy entity through an electronic communication. Pam Dixon of the World Privacy Forum noted after the Premera medical information data breach "[t]he Premera hack may also give rise to phishing campaigns, in which criminals e-mail victims in an effort to trick them into giving up even more information about themselves. Because of the nature of the information stolen…it's difficult to detect which e-mails could be fake and which are genuine, she said." *See* Jaikumar Vijayan, *Premera Hack: What Criminals Can Do With Your Healthcare Data*, Cristian Science Monitor (Mar. 20, 2015), http://www.csmonitor.com/World/Passcode/2015/0320/Premera-hack-What-criminals-can-do-with-your-healthcare-data (last visited September 2, 2016).

(DEA) registration numbers, National Provider Identifiers (NPIs)), [redacted]

29. As a direct and/or proximate result of VAPC's wrongful actions, inaction and/or omissions [redacted], Plaintiffs have suffered (and will continue to suffer) economic damages and injury and harm, including expenditures for protective and remedial services and the costs of monitoring their (and their family's) health and insurance records and financial accounts. Plaintiffs and other patient Class Members also overpaid for the bundled medical care and security services they purchased as their information was not properly secured. Thus, Plaintiffs, on behalf of the Class, request damages to compensate for all such current and future losses.

30. Plaintiffs allege the voluntary relief measures VAPC is offering to only some Class Members – such as one-year of credit monitoring and identity protection services (although Plaintiffs and their families are not even being provided that relief) – are inadequate to ensure future security of personal and sensitive information for all individuals and entities whose sensitive data was compromised. Thus, Plaintiffs, on behalf of the Class, seek appropriate injunctive relief designed to protect Plaintiffs and Class Members, and ensure against the recurrence of a data breach by adopting and implementing reasonable security data practices to safeguard PII, PCI, and PHI. Plaintiffs and the Class direct VAPC to: (1) encrypt all sensitive PII, PCI, and PHI in all places in which that data is stored; (2) comply with all applicable standards for data security and protection; (3) comply with laws and standards protecting medical data; [redacted] and (4) provide to Plaintiffs and Class Members extended credit monitoring services and identity protection services to protect against all types of identity theft, including medical identity theft.

PARTIES

31. Plaintiff Cade Becher is a resident of Maricopa County, Arizona. Plaintiff Becher is an allowance biller for a local accounting company. On or about August 15, 2016, Plaintiff

Becher received a letter from VAPC informing him that he had been victimized by a cyber-attack that may have affected the security of his PII, PCI, and PHI, including his "name, providers' names, date of service, name of health insurer, insurance identification number, place of treatment, and diagnosis and treatment codes." A copy of this letter is attached hereto as Exhibit A. Like VAPC's press release of August 12, 2016 regarding the data breach, the letter sent to Plaintiff Becher [redacted] does not specify exactly which of Plaintiff Becher's information was stolen. It also does not disclose the names of the providers/employers using its anesthesia and pain management services whose data "may have" been compromised. This lack of information impedes Plaintiff Becher's ability to independently discern [redacted] Plaintiff Becher's information remains at high risk for fraud, including identity theft. Plaintiff Becher sought out, received and paid for services from VAPC in reliance on VAPC's representations that it would safeguard his PII, PCI, and PHI. Had Plaintiff Becher known that VAPC's computer systems and data security practices were inadequate to safeguard his highly sensitive PII, PCI, and PHI, he would not have entrusted his PII, PCI, and PHI to VAPC and would not have sought out, received and paid for services from VAPC. As a result of VAPC's conduct alleged herein, Plaintiff Becher has been forced to take affirmative measures to ensure his PII, PCI, and PHI are protected. Specifically, Plaintiff Becher spent time investigating Experian and LifeLock monitoring services, and on January 10, 2017 he enrolled in the LifeLock Advantage Program, for which he pays $19.99 per month. The LifeLock Advantage Program provides Plaintiff Becher with numerous alerts, including fraud detection alerts, every time he transfers money, opens a new account, etc. As a result, Plaintiff Becher has to spend a significant amount of time investigating each and every alert to make sure that his personal accounts and information are secure. [redacted] the constant monitoring Plaintiff Becher has to engage in as a result thereof have left Plaintiff Becher with stress and anxiety over the security of his personal information, including his credit score. Plaintiff Becher has worked hard to obtain a good credit

score and knows that he will want to rely on it in the future when buying things, such as a bigger house or a new car. Plaintiff Becher is constantly worried that his credit score will be negatively affected [redacted] and has considered seeking professional help to treat his anxiety. Plaintiff Becher's concerns are well founded. [redacted] Plaintiff Becher was notified by his bank that someone from China was trying to access his bank account. Plaintiff Becher has thus been harmed and will continue to be exposed to the risk of identity theft or some other fraud.

32. Plaintiff Melanie R. Chaignot is a resident of Maricopa County, Arizona. On or about August 15, 2016, Plaintiff Chaignot received a letter from VAPC informing her that her minor son had been victimized by a cyber-attack that may have affected the security of his PII, PCI, and PHI, including his "name, providers' names, date of service, name of health insurer, insurance identification number, place of treatment, and diagnosis and treatment codes." A redacted copy of this letter is attached hereto as Exhibit B (the minor child's name has been redacted). Plaintiff Chaignot, while not receiving a letter yet from VAPC in her own name, believes that she too is at risk as she took her minor child for treatment where he received services from VAPC, and filled out VAPC's paperwork requesting her personal medical and financial information for purposes of treating her son, including, *inter alia*, her applicable insurance and payment related information. Thus, Plaintiff Chaignot believes that her PII is at high risk for misuse and fraud. Like VAPC's press release of August 12, 2016 regarding the data breach, the letter sent to Plaintiff Chaignot's son [redacted] does not specify exactly which of Plaintiff Chaignot son's information was stolen, nor which of Plaintiff Chaignot's information was stolen. It also does not disclose the names of the providers/employers using its anesthesia and pain management services whose data "may have" been compromised. This lack of information impedes Plaintiff Chaignot's ability to independently discern what PII, PCI, and PHI "may have" been improperly accessed or taken, and to remediate the consequences of any such access. Plaintiff Chaignot's information remains at high risk for misuse and fraud, including identity theft. Plaintiff

Chaignot sought out, received and paid for services from VAPC in reliance on VAPC's representations that it would safeguard her and her son's PII, PCI, and PHI. Had Plaintiff Chaignot known that VAPC's computer systems and data security practices were inadequate to safeguard her and her son's highly sensitive PII, PCI, and PHI, she would not have entrusted her and her son's PII, PCI, and PHI to VAPC and would not have sought out, received and paid for services from VAPC, for herself or for her son. As a result of VAPC's conduct alleged herein, Plaintiff Chaignot has been forced to take affirmative measures to ensure her PII, PCI, and PHI are protected. Specifically, on December 15, 2016, Plaintiff Chaignot enrolled in a LifeLock Advantage plan for which she pays $16.99 per month. Plaintiff Chaignot has already spent over an hour monitoring her LifeLock account and now spends a significant amount of time checking her bank accounts regularly. [redacted] Plaintiff Chaignot has thus been harmed and will continue to be exposed to the risk of identity theft or some other form of fraud.

33. Plaintiff Janice E. Manz is a resident of Maricopa County, Arizona. On or about August 15, 2016, Plaintiff Manz received a letter from VAPC informing her that she had been victimized by a cyber-attack that may have affected the security of her PII, PCI, and PHI, including "name, providers' names, date of service, name of health insurer, insurance identification number, place of treatment, and diagnosis and treatment codes." Like VAPC's press release of August 12, 2016 regarding the data breach, the letter sent to Plaintiff Manz [redacted] does not specify exactly which of Plaintiff Manz's information was stolen. It also does not disclose the names of the providers/employers using its anesthesia and pain management services whose data "may have" been compromised. This lack of information impedes Plaintiff Manz's ability to independently discern what PII, PCI, and PHI "may have" been improperly accessed or taken, and to remediate the consequences of any such access. Plaintiff Manz's information remains at high risk for fraud, including identity theft. Plaintiff Manz's only source of income is a fixed disability income, and she is unable to afford any out of pocket

expenses to protect herself and her PII, PCI, and PHI from fraud or theft due to this data breach. Plaintiff Manz sought out, received and paid for services from VAPC in reliance on VAPC's representations that it would safeguard her PII, PCI, and PHI. Had Plaintiff Manz known that VAPC's computer systems and data security practices were inadequate to safeguard her highly sensitive PII, PCI, and PHI, she would not have entrusted her PII, PCI, and PHI to VAPC and would not have sought out, received and paid for services from VAPC. As a result of VAPC's conduct alleged herein, Plaintiff Manz has been forced to take affirmative measures to ensure her PII, PCI, and PHI are protected. Specifically, Ms. Manz checks her credit score as provided by her bank on a regular basis, as well as her bank account statements to monitor for thefts. As a result, Plaintiff Manz has spent considerable time investigating her credit scores and monitoring her bank accounts. The constant monitoring has caused stress and anxiety over the security of her personal information, including her credit score. [redacted], Plaintiff Manz has been harmed and will continue to be exposed to the risk of identity theft or some other form of fraud.

34. Plaintiff Megan F. Thomas is a resident of Maricopa County, Arizona. On or about August 15, 2016, Plaintiff Thomas received a letter from VAPC informing her that she had been victimized by a cyber-attack that may have affected the security of her PII, PCI, and PHI, including "name, providers' names, date of service, name of health insurer, insurance identification number, place of treatment, and diagnosis and treatment codes." Like VAPC's press release of August 12, 2016 regarding the data breach, the letter sent to Plaintiff Thomas [redacted] does not specify exactly which of Plaintiff Thomas's information was stolen. It also does not disclose the names of the providers/employers using its anesthesia and pain management services whose data "may have" been compromised. This lack of information impedes Plaintiff Thomas's ability to independently discern what PII, PCI, and PHI "may have" been improperly accessed or taken, and to remediate the consequences of any such access. Plaintiff Thomas's information remains at high risk for fraud, including identity theft. Plaintiff Thomas sought out, received and paid for services from VAPC in reliance on VAPC's representations that

it would safeguard her PII, PCI, and PHI. Had Plaintiff Thomas known that VAPC's computer systems and data security practices were inadequate to safeguard her highly sensitive PII, PCI, and PHI, she would not have entrusted her PII, PCI, and PHI to VAPC and would not have sought out, received and paid for services from VAPC. As a result of VAPC's conduct alleged herein, Plaintiff Thomas has been forced to take affirmative measures to ensure her PII, PCI, and PHI are protected. Specifically, Plaintiff Thomas has spent significant time investigating bank account statements and credit reports. Additionally, Plaintiff Thomas is enrolled in Credit Secure credit monitoring by American Express, for which she pays $14.99 per month. Credit Secure provides Plaintiff Thomas with credit score monitoring, and numerous alerts, including fraud detection alerts, money transfer alerts, new account alerts, etc. As a result, Plaintiff Thomas has spent substantial time investigating her credit scores and monitoring her bank accounts. The constant monitoring has caused stress and anxiety over the security of her personal information. Plaintiff Thomas is constantly worried that her credit score will be negatively affected [redacted], Plaintiff Thomas has been harmed and will continue to be exposed to the risk of identity theft or some other form of fraud.

35. VAPC is a group of 300 anesthesiology and interventional pain management providers. VAPC is incorporated in Arizona and has its principal place of business in Maricopa County, Arizona.

JURISDICTION AND VENUE

36. This Court has subject matter jurisdiction over this matter under A.R.S. §12-123 because VAPC is a corporation organized and existing under the laws of the state of Arizona, and maintains its principal executive office in Phoenix, Arizona. Federal jurisdiction does not exist under the Class Action Fairness Act because the local controversy exception applies. Specifically, Plaintiffs are informed and believe that more than two-thirds of the proposed Class Members are citizens of Arizona. Additionally, the "principal injuries" resulting from VAPC's conduct alleged herein were incurred in Arizona. Plaintiffs are also informed and believe that no class action

asserting similar factual allegations has been filed against VAPC in the preceding three years. Finally, as noted below, VAPC is a citizen of Arizona, and Plaintiffs and the proposed Class seek significant relief from VAPC, whose conduct is a "significant basis" of their claims. Alternatively, the home state exception to CAFA applies because two-thirds or more of the members of the proposed class and the Defendant, VAPC, are citizens of Arizona.

37. Venue is proper in this Court under A.R.S. § 12-401 because Defendant VAPC: (1) maintains its principal place of business in this County; (2) conducts executive decisions relating to the collection, retention, security, and dissemination of personally identifiable information, health information, financial information, and provider information of putative Class Members in this County; (3) upon information and belief, retains and "secures" all or most electronically stored personally identifiable information, health information, financial information, and provider information of putative Class members in Arizona; (4) upon information and belief, has all or most relevant VAPC data security team members and information technology staff located in Arizona, and makes all relevant decisions related to data security in Arizona; and (5) has engaged in the activities that gave rise to this complaint in this County.

38. The principal injuries, including the collection, retention, and unlawful access of putative class members' personally identifiable information, health information, financial information, and provider information took place in Maricopa County, Arizona.

FACTUAL ALLEGATIONS

A. Stolen PII, PCI and PHI Provide a Profitable Business for Cyber Thieves Resulting in Extremely Grave Consequences for Victims.

39. Personal and financial information is a valuable commodity.[3] It is so valuable that a "cyber black-market" exists in which criminals openly post stolen data, including financial information, Social Security numbers, health and medical insurance information, and other personal identifying information on a number of Internet websites. Once information is disclosed on the "cyber black-market" it can remain there and continues to be traded for several years.

40. The information compromised in a data breach, [redacted], is significantly more valuable to a cyber attacker than credit card information obtained in a large retailer data breach. Martin Walter, senior director at cyber security firm RedSeal, explained, "Compared to credit card information, personally identifiable information and Social Security numbers are worth more than 10x on the black market."[4]

41. As reported by the Identity Theft Protection Association, "the 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."[5]

---

[3] *See, e.g.,* John T. Soma *et al, Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets*, 15 RICH. J.L. & TECH. 11, at *3-4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted), http://jolt.richmond.edu/v15i4/Article11.pdf (last visited September 2, 2016).

[4] *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-for10x-price-of-stolen-credit-card-numbers.html (last visited September 2, 2016).

[5] Barnett, Michael. *The Internet Information Black Market*, http://businessidtheft.org/Education/BusinessIDTheftScams/InternetBlackMarket/tabid/l 17/Default.aspx (last visited September 2, 2016).

42. In 2013, the EMC²/RSA White Paper noted the profitability of PII, PCI and PHI: "Cyber criminals are selling the information on the black market at a rate of $50 for each partial EHR [electronic health record], compared to $1 for a stolen social security number or credit card number. EHR can then be used to file fraudulent insurance claims, obtain prescription medication, and advance identity theft. EHR theft is also more difficult to detect, taking almost twice as long as normal identity theft."[6]

43. 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.[7] Mr. Gregg further explained that detailed medical records with unique patient identifying numbers can cost as much as $100 per record. *Id*.

44. Once PII, PCI, and PHI are stolen and sold on the black-market, the consequences to the victims are gravely serious: "A thief may use your name or health insurance numbers to see a doctor, get prescription drugs, file claims with your insurance provider, or get other care. If the thief's health information is mixed with yours, your treatment, insurance and payment records, and credit report may be affected."[8]

45. Victims of data breaches, [redacted], will suffer, or are at

---

[6] *See* FBI Cyber Division, Private Industry Notification #140408-009, "Health Care Systems and Medical Devices at Risk for Increased Cyber Intrusions for Financial Gain," (Apr. 8, 2014), http://www.aha.org/content/14/140408--fbipin-healthsyscyberintrud.pdf (last visited September 2, 2016).

[7] Ken Alltucker, *Banner Health Cyberattack Breaches up to 3.7 Million Records,* Ariz. Cent. (Aug. 3, 2009), http://www.azcentral.com/story/money/business/health/2016/08/03/banner-health-cyberattack-breaches-up-3-7-million-records/88035474/ (last visited September 2, 2016).

[8] *See Medical Identity Theft,* Federal Trade Commission, http://www.consumer.ftc.gov/articles/0171-medical-identity-theft (last visited Nov. 15, 2016).

imminent risk of further suffering, identity theft and medical identity theft. As Pam Dixon of the World Privacy Forum explained, "[w]hen someone has your clinical information, your bank account information, and your Social Security number, they can commit fraud that lasts a long time. Th[is] kind of identity theft . . . is qualitatively and quantitatively different than what is typically possible when you lose your credit card or Social Security number."[9] "Not only is this information being traded on the black market for people to commit identity theft, it's also being used to obtain prescription drugs and commit insurance fraud. For the individuals whose identities are used to perpetrate these crimes, their own medical treatments may be impacted, their health insurance disrupted, and their credit scores lowered." *Id*.

46. Victims of data breaches, [redacted], will face many other potential issues. For example, victims face imminent risk of health insurance discrimination—denial of coverage, improper "redlining," and denial or difficulty obtaining disability or employment benefits because information was improperly disclosed to a provider.

47. Victims of data breaches, [redacted], are also particularly susceptible to tax return fraud. It is estimated that in 2016, there will be $21 billion in losses due to fraudulent tax refunds, and data breaches are a large factor contributing to this reality. The U.S. Treasury Inspector General for Tax Administration has recognized that "[t]he increasing number of data breaches in the private and public sectors means more personal information than ever before is available to unscrupulous individuals."[10]

48. Further, victims of retailer breaches – unlike a healthcare data breach, like the [redacted] – can avoid much of the potential for future harm by cancelling credit or debit cards and obtaining replacements. [redacted]

---

[9] *See*, Vijayan, *supra*.

[10] Susan Tompor, *Tax refund losses could reach $21B this year*, http://www.freep.com/story/money/personal-finance/susan-tompor/2016/04/18/tax-refund-losses-could-reach-21b-year/83023206/ (last visited September 2, 2016).

[redacted]

B. The Healthcare Industry Has Been Warned That It is a Prime Target for Cyberattacks and Should Be Diligent in Protecting All Data.

49. According to the U.S. Department of Health and Human Services, data from more than 120 million people has been compromised in more than 1,100 separate breaches at organizations handling protected health data since 2009.[11] Following the Anthem and Premera data breaches, Rachel Seeger, a spokesperson for the Department of Health and Human Services Office for Civil Rights, said in a statement: "We are certainly seeing a rise in the number of individuals affected by hacking/IT incidents, . . . [and] . . . [t]hese incidents have the potential to affect very large numbers of health care consumers." *Id*. And, in its 2015 Study, the Ponemon Institute, an independent cyber-security research institution, reported that "[s]ince last year's study, medical identify theft incidents increased 21.7 percent."[12]

50. Thus, as the frequency of cyber-attacks continues to rise and impact more individuals and volumes of data, especially health and medical related data. There remains an ever-growing need to protect individuals' personal and confidential medical and financial information.

51. Healthcare organizations have been on notice of the threat of cyber-attacks for years. In February 2014, the United States Federal Bureau of Investigation issued a Private Industry Notification, warning healthcare providers that their cybersecurity networks were not sufficiently secure compared to the networks of the financial and retail sectors, making healthcare systems even more vulnerable to hackers seeking Americans' personal medical records and health insurance

---

[11] 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), https://www.washingtonpost.com/news/the-switch/wp/2015/03/20/2015-is-already-the-year-of-the-health-care-hack-and-its-only-going-to-get-worse/ (last visited September 2, 2016).

[12] *See* Ponemon Institute LLC, *Fifth Annual Study on Medical Identify Theft*, at 1 (Feb. 2015), http://medidfraud.org/wp-content/uploads/2015/02/2014_Medical_ID_Theft_Study1.pdf (last visited September 2, 2016).

data.[13] The FBI's warning relied, in part, on findings from three independent, reputable organizations concerned with cyber-security:

- A SANS Institute report (2/2014), "indicat[ing] health care security strategies and practices are poorly protected and ill-equipped to handle new cyber threats exposing patient medical records, billing and payment organizations, and intellectual property."
- A Ponemon Institute report (3/2013), stating that "63% of the health care organizations surveyed reported a data breach in the past two years with an average monetary loss of $2.4 million per data breach" and "45% reported that their [healthcare] organizations have not implemented security measures to protect patient information."
- An EMC²/RSA White Paper (2013), indicating that "in the first half of 2013, over 2 million health care records were compromised, which was 31% of all reported data breaches." The EMC²/RSA White Paper also noted that "EHR theft is also more difficult to detect, taking almost twice as long as normal identity theft." *Id*.

52. As early as 2013 and certainly by 2014, the healthcare industry, including provider groups such as VAPC, were unquestionably aware of the risk of cyber-attacks and the importance of securing PII, PCI, and PHI.

53. The Identity Theft Research Center, a nationally recognized non-profit organization that maintains an extensive database capturing and categorizing U.S. data breaches for purposes of assisting victims and providing consumer education regarding cyber-attacks, reported that in 2015 the "Health/Medical sector" was the second largest industry target of cyber-attacks and accounted for approximately 35.5% of all data breaches throughout the nation.[14]

---

[13] *See* FBI Cyber Division, *supra*.

[14] *Identity Theft Resource Center Breach Report Hits Near Record High in 2015*, Identity Theft Res. Ctr. (Jan. 25, 2016), http://www.idtheftcenter.org/ITRC-Surveys-Studies/2015databreaches.html (last visited September 2, 2016).

54. According to Dave Kennedy, chief executive of information security firm TrustedSEC, cyber criminals target healthcare companies because they maintain large quantities of data possessing significant resale value in black markets. These cyber-criminals exploit security practices that are less sophisticated than those of other industries. As Dave Kennedy has cautioned "[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."[15]

55. The security firm WhiteHat Security recently discovered that within the healthcare industry only about 24 percent of known security flaws are fixed at any given time. On average, healthcare sites take about 158 days to close their vulnerabilities with some flaws remaining unpatched for much longer, said Robert Hansen, vice president of WhiteHat. "That's not good enough", said Mr. Hansen. "Unlike credit card numbers, healthcare information is nonrecoverable, and potentially lethal in the wrong hands," he said.[16]

56. Despite the warnings, VAPC ignored these trends and warnings and repeatedly failed to take adequate and necessary steps to protect patient, consumer, and employee confidentiality and maintain data security.

C. VAPC Requires Disclosure, Collects and Stores PII, PCI and PHI for its Patients, Employees, and Providers, Yet Failed to Take Adequate Measures to Protect It As Required By Federal and State Law.

1. VAPC Requires Disclosure, Collects and Stores PII, PCI and PHI for its Patients, Employees, and Providers

57. VAPC is a group of 300 anesthesiology and interventional pain management providers based in Phoenix, Arizona. In the course of its business, VAPC requests, requires disclosure, retains, and stores patient PII including names, Social Security Numbers, providers'

---

[15] Peterson, *supra*.

[16] Vijayan, *supra*.

names, dates of service, places of treatment, names of health insurers, insurance identification numbers, and diagnosis and treatment codes.

58. VAPC also collects and maintains employee PII/PCI and payment information as a condition of hiring and continued employment. This information includes names, dates of birth, addresses, Social Security Numbers, bank account information, and other financial information.

59. VAPC also collects and maintains provider PII including names, dates of birth, Social Security Numbers, professional license numbers, Drug Enforcement Agency (DEA) numbers, National Provider Identifiers (NPIs), bank account information, and potentially other financial information. In doing so, VAPC was entrusted with, and obligated to safeguard and protect, Plaintiffs' and Class Members' PII/PCI/PHI in accordance with all applicable laws.

60. VAPC is required by law to provide a notice of its privacy practices. 45 C.F.R. §§ 164.520(a) and (b). The notice must describe the ways in which VAPC may use and disclose protected health information; state VAPC's duties to protect privacy, provide a notice of privacy practices, and abide by the terms of the current notice; describe individuals' rights, including the right to complain to HHS and to VAPC if they believe their privacy rights have been violated; and include a point of contact for further information and for making complaints to VAPC. *See* 45 C.F.R. §164.520(a) and (b).

61. VAPC is required by law to provide the Notice of Privacy to all patients when they first enter contractual relationships with VAPC and before patients receive services from VAPC, *see* 45 C.F.R. § 164.520(c)(2)(1), and the notice is incorporated by reference in VAPC's patient registration forms. It thus forms part of the contract between VAPC and the patients who receive services from VAPC.

62. Upon information and belief, VAPC uses a joint privacy practices notice with some of the medical facilities it contracts with, wherein VAPC agrees to abide by the notice content with respect to the protected health information created or received in connection with participation in the arrangement. *See* 45 C.F.R. § 164.520(d). Upon information and belief, such joint notice is

distributed by the medical facility at the first point of contact with the patient and constitutes notice of VAPC's Notice of Privacy. [redacted] Exhibit C [redacted]

63. VAPC is also required by law to prominently post its Notice of Privacy on its web site and make the notice available electronically through the web site. *See* 45 C.F.R. § 164.520(c)(3).

64. VAPC has posted the Notice of Privacy online since at least September 2014. On its website, [redacted] continuing to this day, VAPC expressly states in its "Notice of Privacy" that Plaintiffs and Class Members should expect the following:

> We are required by law to maintain the privacy of your protected health information (PHI). We will let you know promptly if a breach occurs that may have compromised the privacy or security of your PHI.
> * * *
> [E]xcept as stated in this notice, we will not use or disclose your PHI without your written authorization.
> * * *
> **Right to Request Restrictions on Uses and Disclosures**
> You have the right to request that we limit the use and disclosure of your PHI for treatment, payment or health care operations; to persons involved in your care; or for notification purposes as set forth in this notice. . . .

See Notice of Privacy Practices, Valley Anesthesiology & Pain Consultants, https://www.valley.md/pdf/noticeofprivacypractices.pdf (last accessed Sep. 14, 2016).

65. VAPC promises that it is "committed to maintaining the privacy and security of our patients' information." *See Notice to Our Patients Regarding Network Access Incident*, Valley Anesthesiology & Pain Consultants, https://www.valley.md/securityupdate (last visited Sep. 14, 2016).

66. VAPC is also required by law to post the Notice of Privacy in a clear and prominent location at all of its physical services delivery sites. *See* 45 C.F.R. § 164.520 (c)(2)(ii)(B).

67. VAPC is also required by law to make a good faith effort to obtain written acknowledgement from patients of the receipt of the privacy notice. *See* 45 C.F.R. § 164.520 (c).

68. Upon information and belief, VAPC's privacy policies as to employees and providers are substantively analogous to the privacy policies for patients, and are incorporated into the employee handbook VAPC provides to employees and health care providers.

69. Plaintiffs and other Class Members relied on VAPC's promises to maintain the privacy and security of their PII, PCI and PHI when they decided to seek out, receive, and pay for services – including cyber-security services – from VAPC.

2. VAPC's Obligations Under Federal and State Law and Industry Guidelines

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

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

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

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

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

75. During the relevant time period, HIPAA obligated VAPC to protect against any reasonably anticipated threats or hazards to the security or integrity of electronic protected health information. *See* 45 C.F.R. §§ 164.306(a)(2), 164.308.

76. During the relevant time period, HIPAA also obligated VAPC to implement policies and procedures to prevent, detect, contain, and correct security violations, *see* 45 C.F.R. §§ 164.306(a)(1), 164.308, and to protect against uses or disclosures of electronic protected health information that are reasonably anticipated but not permitted by the privacy rules, *see* 45 C.F.R. §§ 164.306(a)(3), 164.308.

77. During the relevant time period, HIPAA obligated VAPC to ensure that its workforce complied with HIPAA security standard rules, *see* 45 C.F.R. §§ 164.306(a)(4), 164.308, to effectively train its workforce on the policies and procedures with respect to protected health information, as necessary and appropriate for those individuals to carry out their functions and maintain the security of protected health information, 45 C.F.R. § 164.530(b)(1).

78. The Office for Civil Rights ("OCR"), within HHS, issues guidance to assist HIPAA-covered entities.[17] For example, the guidance regarding Risk Analysis clarifies the expectations of

---

[17] *See* US Department of Health & Human Services, Security Rule Guidance, http://www.hhs.gov/hipaa/for-professionals/security/guidance/index.html (last visited March 9, 2017).

organizations required to meet the Security Rule requirements, including by providing information on risk analysis requirements, elements of risk analysis, and a list of resources for covered entities to access.[18] The list of resources includes a link to guidelines set by the National Institute of Standards and Technology ("NIST"), which OCR says "represent the industry standard for good business practices with respect to standards for securing e-PHI."

79. Since February 2014, NIST has provided a Framework for Improving Critical Infrastructure Cybersecurity. *See* National Institute of Standards and Technology, Framework for Improving Critical Infrastructure Cybersecurity, February 12, 2014, https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf ("Cybersecurity Framework"). The Cybersecurity Framework provides a voluntary, risk-based approach – based on existing standards, guidelines, and practices – to help organizations to understand, communicate, and manage cybersecurity risks. *See id.*

80. Like HIPAA, the Cybersecurity Framework advises organizations such as VAPC to, *inter alia*: (1) limit access assets and associated facilities to authorized users, processes, or devices, and to authorized activities and transactions, *see* Cybersecurity Framework at PR.AC; (2) provide its personnel and partners with cybersecurity awareness education and adequately train them to perform their information security-related duties and responsibilities consistent with related policies, procedures, and agreements, *see id*. at PR.AT; (3) manage information and records/data consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of the information, *see id.* at PR.DS; and (4) maintain security policies, processes, and procedures and use them to manage protection of information systems and assets, *see id.* at PR.IP.

81. Since September 2013, the International Organization for Standardization ("ISO") and the International Electrotechnical Commission ("IEC") have published an information security

---

[18] See US Department of Health & Human Services, Final Guidance on Risk Analysis, http://www.hhs.gov/hipaa/for-professionals/security/guidance/final-guidance-risk-analysis/index.html (last visited March 9, 2017).

standard which specifies generic requirements for organizations such as VAPC to use in establishing, implementing, maintaining, and continually improving an information security management system as well as requirements for the assessment and treatment of information security risks. See International Organization for Standardization, ISO/IEC 27001:2013, https://www.iso.org/standard/54534.html (last visited March 13, 2017).

82. Like HIPAA and the NIST Cybersecurity Framework, ISO/IEC 27001:2013 advises organizations such as VAPC to, *inter alia*: (1) prevent unauthorized access to systems, services, information, information processing facilities, ensure the security of teleworking and use of mobile devices, and maintain the security of information transferred within an organization and with any external entity, *see* ISO/IEC 27001:2013 at A.6.2, A.9, A.11, A.13; (2) establish management frameworks to initiate and control the implementation and operation of information security within the organization, ensure that employees and contractors understand their responsibilities, are suitable for the roles for which they are considered, and are aware of and fulfill their information security responsibilities, *see id.* at A.6.1.1 and A.7.1 and A.7.2.2; and (3) ensure that information and information processing facilities are protected against malware, protect against the lass of data, ensure that information receives an appropriate level of protection in accordance with its importance to the organization, prevent unauthorized disclosure, modification, removal or destruction of information stored on media, and ensure that information security is an integral part of information systems across the entire lifecycle, *see id.* at A.8.2.3, A.8.3, A.12.2-12.3, A.13.1-13.2, A.14.1.

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

84. Arizona law also requires VAPC to treat Plaintiffs' and Class Members' information confidentially and to protect it from disclosure. Specifically, A.R.S. §§ 36-509 and 36-2221(D) requires VAPC to keep medical records and information confidential.

85. As more fully discussed herein, VAPC failed to comply with its own guidelines, as well as federal, state, and industry guidelines requiring VAPC to take adequate measures to protect the PHI, PCI and PII it collected from patients, providers, and employees. [redacted]

86. Despite its claims that it would "maintain the privacy of [Plaintiffs' and Class Members' PII, PCI and PHI]," on June 13, 2016, VAPC learned that a cyber-attack on its computer systems had taken place on March 30, 2016.

87. VAPC delayed publicly acknowledging the cyber-attack until August 12, 2016 – over four and a half months after the initial attack occurred and two months after it learned of the attack. At that time, VAPC issued a press release notifying affected individuals and entities of the attack and potential security issues regarding their PII, PCI and PHI as set forth in paragraph 14, above. *See Valley Anesthesiology and Pain Consultants Identifies and Addresses Information Security Incident*, PR Newswire (Aug. 12, 2016, 4:00 PM), http://www.prnewswire.com/news-releases/valley-anesthesiology-and-pain-consultants-identifies-and-addresses-information-security-incident-300312986.html.

88. VAPC's Press Release claimed that it "has no evidence that any of the information has been accessed or used inappropriately," and further stated that the forensics firm "was unable to definitively rule that out."[19] [redacted] To date, VAPC has still not confirmed

[19] PR Newswire, *supra*; *see also* Exhibits A-B.

whether the attackers who breached VAPC's computer systems actually obtained any information, [redacted].

90. Upon information and belief, hackers accessed VAPC's computer systems that contain patient, employee, and provider information for putative class members.

91. VAPC stated: "In addition to security safeguards already in place, VAPC is taking steps to enhance the security of its computer systems in order to prevent this type of incident from occurring again in the future. These steps include reviewing its security processes, strengthening its network firewalls, and continuing to incorporate best practices in IT security." However, VAPC has not disclosed precisely what policies VAPC will be developing, and how/when those will actually be implemented to protect the Class. [redacted]

92. The form letters VAPC sent out to affected individuals provide less information [redacted] than the August 12, 2016 press release. And, the letters downplay the likelihood that Plaintiffs and Class Members will experience identity theft or some other harm [redacted] *See, e.g.*, Exhibits A-B.

93. The letter identifies the bare bone details of the timeline of the March 30, 2016 data breach; that patient information ("name, providers' names, date of service, name of health insurer, insurance identification number, place of treatment, and diagnosis and treatment codes") "may" have been on the computer systems at issue and that hackers "may have" gained unauthorized

access to that information; that affected patients should "review the statements they receive" from their insurers to note any potential issues; that VAPC has "established a dedicated call center to answer patients' questions"; and, without providing any information regarding how the breach actually occurred or the exact measures that VAPC will take going forward, that VAPC is "taking steps to enhance the security of our computer systems in order to prevent this type of incident from occurring again in the future", including generally "reviewing our security processes, strengthening our network firewalls, and continuing to incorporate best practices in IT security." *See, e.g.*, Exhibits A-B.

94. Despite its promise that it is "committed to maintaining the privacy and security of our patients' information," (*see, e.g.*, Exhibits A-B), the lack of information provided by VAPC to date regarding this cyber-attack is alarming. VAPC's press release downplayed the significance of the attack and likelihood that Plaintiffs' and Class Members' data may be used for fraudulent purposes. For example, VAPC failed to provide any in-depth or detailed information to the victims as to the actual extent of this compromise, including: [redacted] VAPC also did not urge Plaintiffs and Class Members to take steps to ensure their own personal and financial security, and Class Members complained about the lack of information provided by VAPC regarding what steps they should take to protect themselves and their information. VAPC has not even provided specific information to patients regarding when the compromised data may have been collected or the names of the providers/employers using its

anesthesia and pain management services whose data "may have" been compromised to enable Class Members to independently discern on an individual basis what PII, PCI or PHI may have been improperly accessed. In short, VAPC has placed 100% of the burden on Plaintiffs and Class Members for its failed security practices and, upon information and belief, Class Members have complained to VAPC about the lack of information provided, the lack of and/or insufficient credit monitoring services offered, and [redacted]

95. In its form letter to patients, VAPC fails to state with certainty whether the attackers gained access to private and sensitive patient information – only that they "may" have done so. Then, later in the same letter, VAPC states again that "we have no evidence that any of your information has been accessed or used inappropriately" - without clarification, or disclosure of what effort was made to gather evidence and without disclosing [redacted] VAPC's form letter was not designed to inform but was an attempt to reassure patients and lull them into a false sense of security that there is really nothing to be concerned about. *See* Exhibits A-B.

96. VAPC has even sought to shift the responsibility for ensuring patients' safety onto the patients themselves. For example, in its August 12 letter to Plaintiff, VAPC offered this "guidance on what you can do to protect yourself": "We recommend that you review the explanation of benefits that you receive from your health insurer. If you see services that you did not receive, please contact your insurer immediately." *See* Exhibit A. Further, by failing to identify the many other potential improper uses their PII, PCI and PHI may be subject to, VAPC has

thwarted efforts Class Members may otherwise have taken to protect themselves from these other fraud-related risks.

97. Although VAPC also posted information [redacted] on its website, the notice is titled *Notice to Our Patients Regarding Network Access Incident* – a title which fails to clearly identify to patients, former and current employees and providers what the notice concerns and which those unfamiliar with VAPC may not even pay attention to if they came across it on VAPC's website. *See Notice to Our Patients Regarding Network Access Incident*, Valley Anesthesiology & Pain Consultants, https://www.valley.md/securityupdate (last visited Sep. 2, 2016).

98. While the security measures (or lack thereof) taken by VAPC to prevent this attack, such as lack of appropriate firewalls, were inadequate [redacted] There is no indication that VAPC is approaching and responding to this security failure with the necessary sense of urgency. To date, there is no indication as to whether VAPC has actually implemented security improvements, leaving Plaintiffs' and Class Members' data vulnerable to future data breaches.

99. The form letters sent to Class Members, for example, claim efforts were made to address VAPC's security failures after it learned of the March 30, 2016 breach, [redacted]

[redacted]

E. [redacted]

101. Despite having knowledge of the recent wave of high-profile data breaches and the need for heightened security measures in the wake of large data breaches, such as the widely publicized incidents at Target, Home Depot, Anthem, Premera and others, VAPC failed to develop, implement, and maintain up-to-date data security and retention policies to reduce the risk of cyber-attack and unauthorized release of this information. [redacted]

102. VAPC's failure to develop, implement, and maintain the security of its computer systems and the vast amounts of PII, PCI and PHI it collected, caused the release of Plaintiffs' and Class Members' PII, PCI and PHI. As a result, Plaintiffs and Class Members have an increased likelihood of experiencing identity theft and fraud-related issues in the months and years to come. And, upon information and belief, Plaintiff Becher and other Class Members have already suffered adverse actions [redacted] such as fraudulent attempts (some of them successful) to access bank accounts, fraudulent credit card charges, and out-of-pocket expenses.

103. Plaintiff Becher, [redacted], is concerned that as a result of VAPC's conduct, his PII, PCI and PHI is vulnerable to use by third parties. This concern is well founded, as he was notified [redacted] that someone from China was trying to access his bank account. [redacted], Plaintiff Becher has been forced to expend time and money to guard against further unauthorized access of his accounts, identity theft, and fraud including paying $20 per month for a LifeLock Advantage Program and spending

time monitoring each and every alert that the program sends. [redacted], Plaintiff Becher has suffered from significant stress and anxiety and constantly worries that his personal information will be misused and his credit score, for example, negatively impacted.

104. Plaintiff Chaignot, [redacted], is concerned that as a result of VAPC's conduct, her and her son's PII, PCI and PHI is vulnerable to use by third parties. [redacted], Plaintiff has been forced to expend time and money to guard against further identity theft relating to her and her son's personal information and identity, including paying $16.99 per month for a LifeLock Advantage Program and spending time monitoring her bank accounts. Plaintiff Chaignot is also considering filing a report [redacted] with the Federal Trade Commission (FTC) and/or freezing individual credit reports with each of the three major credit reporting bureaus. [redacted], Plaintiff Chaignot constantly worries that her personal information will be misused.

105. Plaintiff Manz, [redacted], is concerned that as a result of VAPC's conduct, her PII, PCI and PHI is vulnerable to use by third parties. In an effort to protect herself, Plaintiff Manz has spent substantial time to ensure her PII, PCI and PHI are protected.

106. Plaintiff Thomas, [redacted], is concerned that as a result of VAPC's conduct, her PII, PCI and PHI is vulnerable to use by third parties. In an effort to protect herself, Plaintiff Thomas has spent substantial time and money to ensure her PII, PCI and PHI are protected.

107. Plaintiffs' concerns are well founded—according to a 2011 report by Javelin Strategy and Research, individuals who receive a data breach notification letter are more than five times as likely to become victims of identity theft.[20] According to the same report, individuals who

[20] *See* California Office of Privacy Protection, *Recommended Practices on Notice of Security Breach Involving Personal Information* 6 (2012), http://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/recom_breach_prac.pdf (citing Javelin Strategy & Research, *2011 Identity Fraud Survey Report* (2011) (last visited September 2, 2016).

receive a data breach notification letter end up incurring $1,108 of average out-of-pocket costs to remedy a data breach and spend an average of 41 hours resolving the breach, as opposed to $510 and 30 hours for victims who had not received a breach notice. *Id.*

108. The outlay of time and expense is even more extensive when a data breach involves medical identify theft. In its 2015 Study, the Ponemon Institute reported:

> Unlike 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. In some cases, they paid the healthcare provider, repaid the insurer for services obtained by the thief, or they engaged an identity service provider or legal counsel to help resolve the incident and prevent future fraud."[21]

109. The Ponemon Institute reports that "[m]edical identity theft is a complicated crime to resolve" because "on average, victims learn about the theft of their credentials more than three months following the crime and 30 percent do not know when they became a victim. Of those respondents (54 percent) who found an error in their Explanation of Benefits (EOB), about half did not know whom to report the claim to." It becomes even more complicated when an individual is no longer with the insurer with which the EOB has an error – which is the case with Plaintiff Becher.

110. The Ponemon Institute reports "[r]esolution of medical identity theft is time consuming to resolve" because as a result of "HIPAA privacy regulations, victims of medical identity theft must be involved in the resolution of the crime. In many cases, victims struggle to reach resolution following a medical identity theft incident. In our research, only 10 percent of respondents report achieving a completely satisfactory conclusion of the incident. Consequently, many respondents are at risk for further theft or errors in healthcare records that could jeopardize medical treatments and diagnosis." *Id*.

111. "On average, [victims spend] more than 200 hours on such activities as working with their insurer or healthcare provider to make sure their personal medical credentials are secured

---

[21] *See* Ponemon Institute LLC, *Fifth Annual Study on Medical Identify Theft* 1 (2015), http://medidfraud.org/wp-content/uploads/2015/02/2014_Medical_ID_Theft_Study1.pdf (last visited September 2, 2016).

and can no longer be used by an imposter and verifying their personal health information, medical invoices and claims and electronic health records are accurate." *Id.*

112. Due to VAPC's inadequate and unreasonable data security, cyber-criminals have the ability to sell or use Plaintiffs' and putative class members' personal and financial information. To best protect themselves, breach victims must add themselves to credit fraud watch lists, which substantially impair the victims' ability to obtain additional credit.

113. Plaintiffs, as potential victims of identity theft, are struggling to resolve any potential issues, but all of their information can remain available to be misused by identity thieves and others for years into the future.

F. VAPC Failed to Provide Adequate Relief.

114. VAPC is not providing Plaintiffs and the Class with any protection against medical identity theft and fraudulent health insurance claims, the victims of which are often left with huge medical bills, damaged credit, public disclosure of their medical condition, and erroneous medical records.

115. VAPC has not offered sufficient guidance to victims regarding the process of contacting credit reporting agencies to monitor for fraudulent activity. Many Class Members will pay for reporting services that are not needed because they simply do not understand the process. And, upon information and belief, Class Members have purchased LifeLock and other credit monitoring services at a cost of hundreds of dollars [redacted]. Further, the three major credit reporting bureaus maintain websites that can be difficult to navigate for the average user and often unclear as to what is provided as a free service. For example, major credit bureaus may charge approximately $30 to freeze a credit report by default. This charge can be avoided if the filer has previously filed a police report.

116. Even VAPC's offer of free credit monitoring or identity protection services to a limited number of Class Members is woefully inadequate. First, at best, the credit monitoring service is an indirect manner of tracking identity theft – it may reveal new credit accounts opened

with compromised PII/PCI/PHI, but does nothing to prevent unauthorized use of Plaintiffs' and Class Members' PII/PCI/PHI or unauthorized charges to existing payment card accounts.

117. Second, it is unknown how extensive the free credit monitoring and identity protection services being offered by VAPC are. Anything less than several years of monitoring is inadequate, and upon information and belief, Class Members have complained about the minimal length of the services offered by VAPC. The FTC recommends placing an extended fraud alert with each credit reporting agency after your identity has been compromised.[22] These fraud alerts last for seven years. Extended fraud alerts are necessary because when a breach occurs victims' personal, financial, and health information remain accessible by unauthorized parties for years. Often times, hackers will lay low when data breaches are exposed and wait until consumers are less likely to be on the alert of fraudulent activity. The FTC also recommends taking multiple steps once your data has been compromised, including placing a fraud alert, requesting a credit freeze, ordering your credit reports, creating an identity theft report, and filing a police report. Thus, Plaintiffs and the Class must take additional steps to protect their credit and identities, and VAPC has done nothing to assist Class Members with those efforts.

118. Most significantly, VAPC's offer of free credit monitoring is not even being offered to ***all*** Class Members. Patients—of which over 880,000 had their PII/PCI/PHI compromised—are not being offered free credit monitoring or identity protection services at all unless they had their Social Security or Medicare numbers compromised. Thus, for the vast majority of affected Class Members, VAPC is essentially offering no assistance to address the damage [redacted], other than woefully insufficient and incomplete "guidance" on how patients can review their own records. And, Class Members have complained to VAPC about this lack of guidance and discrimination in offering credit monitoring services. [redacted]

[22] Fed. Trade Comm'n, *Taking Charge – What To Do If Your Identity Is Stolen* 9 (2013), https://www.consumer.ftc.gov/articles/pdf-0009-taking-charge.pdf (last visited November 15, 2016.

[redacted]

119. Likewise, compromised provider NPIs and Drug Enforcement Administration ("DEA") numbers are not being addressed by VAPC's free credit monitoring offer, causing providers to have to continually monitor for misuse of this data.

120. Although VAPC claims it is "taking steps to enhance the security of its computer systems" to avoid future breaches, as set forth above, it is unclear precisely what policies it will be developing and how/when those will actually be implemented. [redacted] Plaintiffs and Class Members have a valid concern about VAPC's ability to ensure that similar breaches do not occur in the future.

121. Plaintiffs and Class Members require, and are entitled to, adequate credit monitoring, identity theft insurance, periodic credit reports, and other measures necessary to mitigate the security risks and damage caused by VAPC's failure to properly safeguard their PII, PCI and PHI. VAPC is liable for all associated costs and expenses.

CLASS DEFINITION AND ALLEGATIONS

122. Under Rule 23 of the Arizona Rules of Civil Procedure, Plaintiffs bring this action as a class action on behalf of themselves, and all members of the following Class of similarly situated individuals and entities:

> All persons whose personally identifiable information, health information, bank account information, financial information, or health provider information was stored on VAPC's electronic data systems before August 12, 2016.[23]

123. Excluded from the Class are VAPC, 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

[23] Plaintiffs reserve the right to amend the class definition after discovery.

and associated court staff assigned to this case, and all persons within the third degree of relationship to any such persons.

124. **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, 882,590 patients, and all current and former employees and providers either had their personally identifiable information, heath information, and/or health provider information [redacted]

125. **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 VAPC was negligent in adopting, designing, implementing, or supervising its information technology security systems;

b. whether VAPC violated state laws thereby breaching its duties to Plaintiffs and the Class;

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

d. whether VAPC owed a duty to Plaintiffs and the Class to adequately protect their medical, financial, and personal information;

e. Whether VAPC owed a duty to Plaintiffs and the Class to provide timely and accurate notice [redacted];

f. whether VAPC's conduct, including its failure to act, resulted in or was the proximate cause [redacted] resulting in the loss of patients', employees' and providers' medical, financial, and personal information;

g. whether Plaintiffs and members of the Class suffered injury as a direct and proximate result of VAPC's conduct or failure to act; and

h. whether Plaintiffs and the Class are entitled to recover damages, equitable relief, and other relief, and the extent of the remedies that should be afforded to Plaintiffs and the Class.

126. **Typicality**. Plaintiffs' claims are typical of the claims of the Class. Plaintiffs 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 conduct. While not all aspects of each Class Member's circumstances are identical, the material aspects of their claims are typical.

127. **Adequacy**. Plaintiffs and their counsel will fairly and adequately represent the interests of the Class Members. Plaintiffs have no interests antagonistic to, or in conflict with, the interests of the other Class Members, and they will zealously pursue the claims in this action. Plaintiffs' 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.

128. **Superiority**. A class action is superior to all other available methods for fairly and efficiently adjudicating the claims of Plaintiffs and the Class Members. Plaintiffs and the Class Members have been harmed by VAPC's wrongful actions and/or inaction. Litigating this case as a class action will reduce the possibility of repetitious litigation relating to VAPC'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.

129. 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.

130. The expense and burden of litigation would substantially impair the ability of Plaintiffs and Class Members to pursue individual lawsuits to vindicate their rights on an efficient basis. Absent a class action, VAPC will have wrongfully jeopardized the PII, PCI and PHI of

Plaintiffs and Class Members and shifted the risk of problems and misuse to Plaintiffs and the Class Members. Through the use of effective, long-term credit monitoring and identity protection services, the many effects of VAPC's misconduct can be mitigated or prevented.

131. As to claims for injunctive or declaratory relief, class certification is appropriate under Ariz. R. Civ. P. 23(b)(2) because VAPC has acted or refused to act on grounds generally applicable to the Class, so that final injunctive relief or corresponding declaratory relief is appropriate to the Class as a whole.[24]

COUNT I
NEGLIGENCE

132. Plaintiffs reallege and incorporate all previous allegations.

133. By requesting, requiring, and accepting Plaintiffs' and Class Members' PII, PCI and/or PHI, VAPC assumed a common law duty to Plaintiffs and the Class independent of any contractual duties it assumed to maintain confidentiality and to exercise reasonable care in obtaining, retaining, securing, safeguarding and protecting their medical, financial, and personal information in VAPC's possession from being compromised, lost, stolen, accessed and misused by unauthorized persons. This duty included, among other things, designing, implementing, maintaining, and testing VAPC's security systems to ensure that Plaintiffs' and Class Members' PII, PCI and/or PHI in VAPC's possession was adequately secured and protected.

134. VAPC also had duties that arose from, *inter alia*, state statutes, the Federal Trade Commission Act, and the following HIPAA regulations:

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

---

[24] Plaintiff reserves the right to seek an Ariz. R. Civ. P. 23(c)(4) class or otherwise subclass the class if deemed appropriate after further discovery.

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

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

d. 45 C.F.R. § 164.306(a)(4) for failing to ensure compliance with 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.

135. VAPC breached its duty of care by failing to adequately secure and protect Plaintiffs' and the Class Members' PII, PCI and/or PHI. VAPC had inadequate computer systems and data security practices to safeguard such information.

136. VAPC also had a duty pursuant to A.R.S. § 18-545, [redacted] to provide notice to Plaintiffs and Class Members in the "most expedient manner possible and without unreasonable delay…"

137. VAPC was negligent and negligent per se by breaching its duty to Plaintiffs and Class Members under Arizona law independently from acts in breach of its contractual duties by failing to notify Plaintiffs and Class Members [redacted] in the "most expedient manner possible and without unreasonable delay" and failing to accurately and fully disclose to Plaintiffs and members of the Class that their PII, PCI and/or PHI had been or was reasonably believed to have been compromised. Timely disclosure was required, appropriate, and necessary so that, among other things, Plaintiffs and members of the Class could take appropriate measures to avoid identity theft or medical identity theft if possible.

138. VAPC also had a duty to implement adequate remedial measures to mitigate the risk to Plaintiffs and Class members of identity theft [redacted]

139. VAPC breached its duty to implement adequate remedial measures to mitigate the risk of identity theft independent from acts in breach of its contractual duties by, *inter alia*, failing to immediately implement appropriate remedial [redacted] failing to provide Plaintiffs and Class members any protection against medical identity theft and fraudulent health insurance claims, failing to provide several years' worth of credit monitoring services to Plaintiffs and Class members, not offering sufficient guidance to Plaintiffs and Class members regarding how to navigate the process of contacting the credit reporting agencies, and doing nothing to prevent unauthorized use of Plaintiffs' and Class members' PII/PCI/PHI or unauthorized charges to existing payment card accounts.

140. VAPC's conduct created a foreseeable risk of harm to Plaintiffs and Class Members including, *inter alia*, credit damage, financial loss, and reputational harm.

141. VAPC did not take adequate steps to protect the security of Plaintiffs' and Class Members' PII, PCI and/or PHI.

142. As a direct and proximate result of VAPC's failure to take reasonable care and use reasonable measures to protect the personally identifiable information, credit card information, heath information, or health provider information placed in its care, Plaintiffs and Class Members suffered injury in fact, and will continue to be injured and incur damages because their PII, PCI and PHI was disclosed or acquired by unauthorized parties and their privacy was lost.

143. Plaintiffs and Class Members were not given the opportunity by VAPC to allocate the risk of negligent data security practices as VAPC's contract was offered to Plaintiffs and Class Members on a take it or leave it basis.

144. The Parties' contract does not provide remedies for VAPC's negligence in failing to adequately safeguard and protect Plaintiffs' and Class Members' PII, PCI and PHI, [redacted] and implement adequate remedial measures.

145. Plaintiffs are entitled to recover the damages [redacted] including, *inter alia*, the cost of credit monitoring, identity theft consultation, and identity restoration, as well as the costs related to the detection and prevention of unauthorized use of their financial accounts, including credit monitoring, all of which have an ascertainable money value to be proven at trial.

146. Plaintiffs are also entitled to recover for any credit damage, financial loss, and/or reputational harm resulting from the unauthorized use of their PII, PCI, and PHI [redacted]

COUNT II
VIOLATION OF THE ARIZONA CONSUMER FRAUD ACT,
A.R.S. §44-1521, *et seq.* ("ACFA")
(Applicable to Patients Only)

147. Plaintiffs reallege and incorporate all previous allegations.

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

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

A.R.S. § 44-1522.

149. Plaintiffs and members of the Class are "persons" as defined by A.R.S. § 44-1521(6), VAPC provides "services" as that term is included in the definition of "merchandise" under A.R.S. § 44-1521(5), and VAPC is engaged in the "sale" of "merchandise" as defined by A.R.S. § 44-1521(7).

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

- misrepresenting material facts to Plaintiffs and to the Class, in connection with the sale of health services, by representing at the time that Plaintiffs and Class Members received services from VAPC [redacted] that it would maintain adequate data privacy and security practices and procedures to safeguard Class Members' and Plaintiffs' PII, PCI and/or PHI from unauthorized disclosure, release, data breaches, and theft;
- misrepresenting material facts to Plaintiffs and the Class, in connection with sale of health services, by representing, at the time of providing services to Plaintiffs and the Class [redacted], that VAPC did and would comply with the requirements of the relevant federal and state laws pertaining to the privacy and security of Plaintiffs' and Class Members' PII, PCI and/or PHI;
- failing to disclose [redacted] to Plaintiffs and Class Members in a timely and accurate manner, in violation of A.R.S. § 18-545;
- failing to take proper action [redacted] to enact adequate privacy and security measures, and protect Plaintiffs' and Class Members' PII, PCI and/or PHI from further unauthorized disclosure, release, data breaches, and theft; and

[redacted]

151. In addition, VAPC's failure to disclose that its computer systems were not well-protected, and that Plaintiffs' and Class Members' sensitive information was vulnerable and susceptible to intrusion and cyber-attacks constitutes deceptive and/or unfair acts or practices and material omissions because VAPC knew such facts would: (a) be unknown to and not easily discoverable by Plaintiffs and the Class; and (b) defeat Plaintiffs' and Class Members' ordinary, foreseeable and reasonable expectations concerning the security of VAPC's computer servers.

152. Plaintiffs relied on VAPC's promises to maintain the privacy and security of their PII, PCI and PHI when Plaintiffs decided to seek out, receive, and pay for medical and associated security services from VAPC. Had VAPC disclosed to Plaintiffs that its computer systems were not well-protected, and that Plaintiffs' sensitive information was vulnerable and susceptible to intrusion and cyber-attacks, Plaintiffs would not have entrusted VAPC with their PII, PCI and PHI and would not have received and paid for services from VAPC. Thus, as a result of VAPC's omissions, Plaintiffs' and Class Members were induced to buy bundled medical and security services that they otherwise would not have and overpay for security services they did not receive.

153. VAPC also engaged in unfair acts and practices, in connection with the sale of health services which constitutes "merchandise" under the ACFA by failing to maintain the privacy and security of Plaintiffs' and Class Members' personal information, in violation of duties imposed by and public policies reflected in applicable state laws, Arizona Insurance Information and Privacy Protection Act (A.R.S. § 20-2113), [redacted]

154. VAPC intended that Plaintiffs and the Class rely on its deceptive and/or unfair acts and practices, misrepresentations, and the concealment, suppression, and omission of material facts, in connection with VAPC's offering of medical services and incorporating Plaintiffs' and Class Members' PII, PCI and/or PHI on its computer servers, in violation of the ACFA.

155. VAPC's wrongful practices occurred in the course of trade or commerce.

156. VAPC's wrongful practices were and are injurious to the public interest because those practices were part of a generalized course of conduct that applied to Plaintiffs and all Class Members, and were repeated continuously before and after VAPC obtained PII, PCI and/or PHI concerning Plaintiffs and Class Members. All Class Members have been adversely affected by VAPC's conduct and the public was and is at risk as a result thereof.

157. VAPC's unfair and/or deceptive conduct proximately caused Plaintiffs' and Class Members' injuries because, had VAPC maintained the sensitive information with adequate security, Plaintiffs and the Class Members would not have had it compromised or stolen.

158. Plaintiffs and the Class seek actual damages, compensatory, punitive damages, injunctive relief, and court costs and attorneys' fees as a result of VAPC's violations of the ACFA.

COUNT III
BREACH OF CONTRACT

159. Plaintiffs reallege and incorporate all previous allegations.

160. All contracts between Plaintiffs and Class Members and VAPC were entered into prior to [redacted] August 12, 2016.

161. As a condition of receiving treatment, employment, or acting as a medical provider, VAPC requested Plaintiffs' and Class Members' PII, PCI and/or PHI. Plaintiffs and Class Members provided that information to VAPC in accordance with VAPC's contractual requirements.

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

163. As set forth above, all Plaintiffs and Class Members who were employed by VAPC entered into contracts that included, either by express provision or attachment, or incorporation by reference, VAPC's then-current privacy policies pertaining to employees' and health care providers' personally identifiable information, including but not limited to employee handbooks and workforce confidentiality policies.

164. VAPC promised to maintain the privacy of Plaintiffs' and Class Members' PII, PCI and PHI.

165. VAPC also was required by law to maintain the privacy of Plaintiffs' and Class Members' PHI, PCI and PII, as provided in VAPC's own documents (including its Notice of Privacy), and federal, and state law as alleged above, such as HIPAA and the Federal Trade Commission Act.

166. It was also an implied term of the parties' contract that VAPC was required to maintain the privacy of Plaintiffs' and Class Members' PHI, PCI and PII, and some portion of Plaintiffs' and Class Members' payments to VAPC was directed to maintaining the privacy of their PII, PCI and PHI.

167. Securing Plaintiffs' and Class Members' PII, PCI and PHI was a justified expectation under the contract because of its promises to do so, as well as state and federal laws requiring Defendant to secure PII, PCI and PHI.

168. How best to secure Plaintiffs' and Class Members' PII, PCI and PHI was left to VAPC's discretion under the contract. VAPC breached the covenant of good faith and fair dealing by failing to exercise its discretion in good faith by choosing security measures that were woefully inadequate despite the well-known and obvious threat of attack by cyber criminals.

169. Plaintiffs and Class Members fully performed their duties under the contract, including paying for bundled medical and security services, except to the extent their duties were excused or prevented.

170. VAPC breached its contractual duties when it failed to protect Plaintiffs' and the Class Members' PII, PCI and/or PHI.

171. As a natural and probable consequence of VAPC's breach of contract, Plaintiffs' and Class Members' PII, PCI and/or PHI was disclosed to unauthorized parties leaving Plaintiffs 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.

172. Because of VAPC's breach of contract, Plaintiffs and the Class have suffered injury in fact, including loss of privacy and monetary damages by the unauthorized disclosure or theft of their PII, PCI and/or PHI and are entitled to recover damages, including all costs associated with mitigating their damages through the detection and prevention of identity theft, including credit monitoring, identity theft consultation, and identity restoration.

173. Also as a result of VAPC's failure to implement the security measures required by the contracts, Plaintiffs and Class Members did not receive the benefit of their bargain, and instead received services that were less valuable than what they paid for in reliance on their contracts with VAPC.

174. Plaintiffs and the Class are entitled to recover attorneys' fees and costs pursuant to A.R.S. §12-341.01.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, individually and on behalf of all others similarly situated, pray:

A. That the Court certify this case as a class action and appoint Plaintiffs Becher, Chaignot, Manz, and Thomas as class representatives and Hagens Berman Sobol Shapiro LLP and Bonnett, Fairbourn, Friedman, & Balint, P.C., as co-lead class counsel;

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

C. That the Court award Plaintiffs and the Class appropriate monetary relief, including actual damages, and restitution;

D. That the Court award Plaintiffs and the Class equitable, injunctive and declaratory relief as maybe appropriate;

E. That the Court award attorneys' fees to Plaintiffs' counsel and an incentive award for Plaintiffs, each in an amount deemed reasonable by this Court; and

F. That the Court award Plaintiffs and the Class such other relief as may be available and appropriate.

DATED: March 31, 2017

BONNETT, FAIRBOURN, FRIEDMAN & BALINT, P.C.

By *s/Elaine A. Ryan*
Elaine A. Ryan (012870)
Carrie A. Laliberte (032556)
2325 E. Camelback Road, Suite 300
Phoenix, Arizona 85016
Tel: 602-274-1100
Fax: 602-274-1199
eryan@bffb.com
claliberte@bffb.com

BONNETT, FAIRBOURN, FRIEDMAN & BALINT, P.C.
Patricia N. Syverson (AZ Bar 020191)
Manfred M. Muecke (*To be Admitted Pro Hac Vice*)
600 W. Broadway, Suite 900
San Diego, California 92101
Tel: 619-798-4593

psyverson@bffb.com
mmuecke@bffb.com

HAGENS BERMAN SOBOL SHAPIRO LLP
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
rob@hbsslaw.com
leonard@hbsslaw.com
michellak@hbsslaw.com

WESTERMAN LAW CORP.
Jeff S. Westerman
1875 Century Park East, Suite 2200
Los Angeles, CA 90067
Tel: 310-698-7880
Fax: 310-755-9777
jwesterman@jwslegal.com

EMERSON SCOTT, LLP
John G. Emerson (*Admitted pro hac vice)*
jemerson@emersonfirm.com
David G. Scott
dscott@emersonfirm.com
830 Apollo Lane
Houston, TX 77058
Tel: 281- 488-8854
Fax: 281- 488-8867

Counsel for Plaintiffs and the Proposed Class

ORIGINAL efiled on March 31, 2017

COPY emailed March 31, 2017 to:

COPPERSMITH BROCKELMAN PLC
Keith Beauchamp (012434)
Shelley Tolman (030945)
2800 North Central Avenue, Suite 1200
Phoenix, Arizona 85004
T: (602) 381-5490
F: (602) 224-0999
kbeauchamp@cblawyers.com
stolman@cblawyers.com

Paul G. Karlsgodt, admitted *pro hac vice*
Casie D. Collignon, admitted *pro hac vice*
Baker & Hostetler LLP
1801 California Street, Suite 4400
Denver, CO 80202-2662
pkarlsgodt@bakerlaw.com
ccollignon@bakerlaw.com

Attorneys for Defendant

/s/*Teresa DiNardo*