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

GRANT WOODS P.C.
J. Grant Woods (006106)
Two Renaissance Square
40 N. Central Avenue, Suite 2250
Phoenix, AZ 85004
Telephone: (602) 258-2599
Facsimile: (602) 258-5070
E-mail: gw@grantwoodspc.net

Attorneys for Plaintiff

THE SUPERIOR COURT OF THE STATE OF ARIZONA

IN AND FOR THE COUNTY OF MARICOPA

JASON LIEBICH, individually and on behalf of all other similarly situated,

Plaintiff,

vs.

MARICOPA COUNTY COMMUNITY COLLEGES DISTRICT,

Defendant.

No. CV2014-006870

CLASS ACTION COMPLAINT

(Assigned to _____)

Plaintiff, Jason Liebich, individually and as class representative on behalf of all similarly situated persons and the general public, brings this action against Maricopa County Community Colleges District ("MCCCD") and alleges as follows:

I. INTRODUCTION

1. A community college district that requests for its own purposes and then retains millions of individuals' personal information must ensure that the information is safeguarded from theft, especially when the district is put on notice that its security measures are insufficient and that the personal information is at risk of theft or hacking. When a data breach affecting at least 2.5 million current and former students, employees, and vendors occurs, those students, employees, and vendors must be notified immediately of unauthorized access to their information so they may act to prevent financial losses arising out of the misuse of stolen personal and financial information. This lawsuit stems from MCCCD's failure on both accounts.

2. MCCCD is a community college district operating ten community colleges and two skill centers in Maricopa County, Arizona. MCCCD currently has over 265,000 students and over 9,500 employees. In the 2012-2013 period, MCCCD had over $1.5 billion in revenue.

3. Beginning in at least January 2011, and continuing through November 27, 2013, several of MCCCD's databases were breached and made available for sale on the internet. The breach affected over 2.5 million current and former students, employees, and vendors.

4. The MCCCD data breach could have been prevented. In January 2011, MCCCD was specifically warned by the FBI that several of its databases had been breached and made available for sale on the internet. MCCCD employees were independently aware of this security breach at the time. Even though MCCCD was aware of the breach, it failed to implement any changes or take any actions to secure those databases. This failure to act resulted in a second breach in 2013. On April 29, 2013, the FBI informed MCCCD that fourteen of its databases had been breached and made available for sale on the internet. Despite the 2011 warning, MCCCD did not make any significant changes, and certainly did not take the action necessary to prevent further data incursions by unauthorized persons.

5. To make matters worse, MCCCD failed to promptly disclose the data breach and failed to notify victims of the data breach in a reasonable or timely manner. MCCCD waited over six months, until November 27, 2013, to inform its current and former students, employees, and vendors that the data system was breached and their personally identifiable information may have been sold and exploited.

6. As a result of the MCCCD data breach, the names, addresses, phone numbers, email addresses, Social Security Numbers, dates of birth, financial and bank account information, demographical information, information related to employment, education, and training, benefits information, academic information, financial aid information, and Federal Employer Identification Numbers have been exposed to fraud and these individuals have been harmed as a result. The harm to victims of the MCCCD data breach includes expenses related to credit monitoring, credit restoration, and identity theft prevention, and the time and inconvenience of dealing with issues resulting from the unauthorized disclosure of personal information. Plaintiff seeks to remedy these harms, and prevent their future occurrence, on his behalf and on behalf of all victims of the MCCCD data breach.

II. PARTIES, JURISDICTION AND VENUE

7. Plaintiff Jason Liebich is a resident of Maricopa County, Arizona.

8. MCCCD is a state agency operating in Maricopa County, Arizona.

9. Plaintiff served a notice of claim on MCCCD on March 4, 2014, pursuant to A.R.S. § 12-821.01. MCCCD denied Plaintiff's notice of claim in writing on April 14, 2014.

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

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

III. FACTS

A. MCCCD Collects and Stores Personal Information for its Current and Former Students, Employees, and Vendors.

12. MCCCD collects and maintains information on former and current students, former and current employees, and former and current vendors.

13. MCCCD publishes a policy entitled "Best Practices for Data Security, Acceptable Use and Access Management" ("the Best Practices policy"). This policy has been in effect since July 1, 2007.

14. According to MCCCD's Best Practices policy, MCCCD "[r]ecognizes its affirmative and continuing need to protect confidential employee and student data and to maintain the confidentiality of that data."

15. By its own terms, MCCCD's Best Practices policy was designed to:

a. Ensure the security and protection of confidential information in its custody, whether in electronic, paper, or other forms;

b. Protect against any anticipated threats or hazards to the security or integrity of such confidential information; and

c. Protect against unauthorized access to or use of such confidential information.

16. MCCCD's Best Practices policy further states, "While access and use of data is essential to accomplishing the MCCCD's institutional mission, it further requires the observance of critical standards to safeguard individuals' rights that are protected by state and federal laws or MCCCD regulations."

17. MCCCD's Best Practices policy charges, "[a]ll employees and agents of MCCCD and anyone working on behalf of MCCCD . . . with the protection of MCCCD data."

18. MCCCD's Best Practices policy references another policy, titled "Reasonable Protection."

19. MCCCD's Reasonable Protection policy specifically addresses storing data, and provides, "Confidential data should be stored or made available in such a way that access is restricted and authorization required prior to presenting such data to authorized persons or processes."

20. MCCCD's policy further provides that MCCCD may use "firewalls, restricted or private networks, physical access security or other techniques or systems designed to stop or mitigate the success of unauthorized attempts to obtain data."

21. MCCCD's Best Practices Policy maintains that MCCCD is compliant with state and federal legislation, including FERPA, the Gramm-Leach-Bliley Act, Federal Trade Commission Regulations (16 CFR, Part 314), Standards for Safeguarding Customer Information, HIPAA, and A.R.S. § 15-141.

22. MCCCD was not compliant with these state and federal standards.

23. For example, the FTC's guidelines provide that " to develop, implement, and maintain your information security program," an entity shall:

a. Designate an employee or employees to coordinate your information security program.

b. Identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that could result in the unauthorized disclosure, misuse, alteration, destruction or other compromise of such information, and assess the sufficiency of any safeguards in place to control these risks. At a minimum, such a risk assessment should include consideration of risks in each relevant area of your operations, including:

    1. Employee training and management;

    2. Information systems, including network and software design, as well as information processing, storage, transmission and disposal; and

    3. Detecting, preventing and responding to attacks, intrusions, or other systems failures.

c. Design and implement information safeguards to control the risks you identify through risk assessment, and regularly test or otherwise monitor the effectiveness of the safeguards' key controls, systems, and procedures.

d. Oversee service providers, by:

1. Taking reasonable steps to select and retain service providers that are capable of maintaining appropriate safeguards for the customer information at issue; and

2. Requiring your service providers by contract to implement and maintain such safeguards.

e. Evaluate and adjust your information security program in light of the results of the testing and monitoring required by paragraph (c) of this section; any material changes to your operations or business arrangements; or any other circumstances that you know or have reason to know may have a material impact on your information security program.

16 C.F.R. § 314.4.

24. These regulations create an industry standard for school districts like MCCCD, but, as shown below, MCCCD failed to implement and follow these standards.

B. MCCCD Knew Its ITS System Was Breached in 2011 But Failed to Remedy the Breach or Notify the Affected Individuals.

25. MCCCD was aware in January 2011 that its servers and databases were not secure.

26. In January 2011, MCCCD Information Technology Services ("ITS") employees discovered that MCCCD databases had been breached and made available for sale on the internet.

27. ITS employees also discovered that MCCCD's system had been hacked and contained viruses.

28. At least two of MCCCD's ITS employees were tasked with fixing these problems.

29. As part of that effort, these ITS employees continually reported the ongoing issues to Vice Chancellor George Kahkedjian.

30. In January 2011, the FBI similarly informed MCCCD ITS that one or more of MCCCD's databases had been breached and made available for sale on the internet.

31. MCCCD reported that after the FBI informed them it of the breach, it began an internal investigation.

32. In early 2011, MCCCD also hired outside security consultants Stach & Lui (now Bishop Fox) to conduct an investigation.

33. Stach & Lui issued a report to MCCCD sometime in 2011, identifying significant security vulnerabilities in MCCCD's data systems.

34. In November 2011, MCCCD employees also delivered an internal report, titled "ITS Oversight Report," to Vice Chancellor George Kahkedjian, which identified the ongoing security risks and vulnerabilities in the MCCCD servers.

35. This report noted that MCCCD servers had been hacked and MCCCD continued to run on a compromised server.

36. Despite these reports and MCCCD's knowledge of the breach, MCCCD failed to remedy the data breach, failed to secure its servers, and failed to address the security vulnerabilities identified by MCCCD employees or by Stach & Lui.

37. MCCCD also failed to notify the affected students, employees, and vendors that their personal information was likely compromised and was not secure.

38. Upon information and belief, MCCCD Vice Chancellor Kahkedjian was aware of the data breach in 2011 and failed to take sufficient actions to remedy the breach or secure MCCCD's servers.

39. On October 12, 2012, at least two MCCCD ITS employees filed a formal grievance with the MCCCD Chancellor, Rufus Glasper, and Vice Chancellor Kahkedjian. The grievance mentions the 2011 ITS Oversight Report as well as other problems in the ITS department.

C. MCCCD Was Informed In Early 2013 of the Ongoing Security Breach But Again Failed to Notify the Affected Individuals.

40. On April 29, 2013, the FBI informed MCCCCD that fourteen of its databases had been breached and made available for sale on the internet. The databases were located on MCCCD web servers.

41. After receiving the second notice from the FBI, MCCCD finally took the compromised servers, as identified by the FBI, offline.

42. MCCCD then retained outside counsel, Wilson Elser Moskowitz Edelman & Dicker LLP ("Wilson").

43. Wilson retained Kroll Advisory Services ("Kroll") to investigate the data breach and the failure of MCCCD to act following the 2011 data breach.

44. The compromised data systems contained the following information, which constitutes "Personally Identifiable Information" or "PII":

a. for current and former students, names, addresses, phone numbers, email addresses, Social Security Numbers, dates of birth, certain demographical information, and enrollment, academic, and financial aid information;

b. for current and former employees, names, addresses, phone numbers, email addresses, Social Security Numbers, dates of birth, financial and bank account information, certain demographical information, information related to employment, education, and training, and benefits information, including plan selection, vacation accrual, and dependent information; and

c. for current and former vendors, names, business names, addresses, Federal Employer Identification Numbers, and bank account information.

45. Although MCCCD was aware that these servers could have been accessed by a third party and MCCCD's databases were for sale on the internet, it did not immediately notify the affected individuals, but instead waited seven months to issue any kind of notification.

46. Kroll finished its investigation on October 18, 2003, but could not definitively determine whether any PII was improperly accessed or taken from MCCCD's servers. Kroll did determine that PII could have been improperly accessed or taken.

47. Even after MCCCD received Kroll's report, MCCCD waited more than a month to announce the data breach to the public.

48. MCCCD finally announced the data breach on November 28, 2013, seven months after receiving notice of the latest breach and almost three years after it first learned its systems were not secure.

49. MCCCD also began notifying current and former students, employees and vendors that their Personally Identifiable Information had been compromised on November 27, 2013.

50. As part of that notification, MCCCD began mailing notices to some current and former students, employees, and vendors.

51. As part of that notification, MCCCD offered to provide one year of credit monitoring and credit restoration with Kroll.

52. As of April 15, 2014, MCCCD was falsely advising class members that no data breach had occurred, including current students who were never informed (in writing or otherwise) that a data incursion had occurred.

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

53. Jason Liebich is a current student at Phoenix College, one of MCCCD's ten community colleges.

54. Mr. Liebich applied to attend classes at Phoenix College in late 2011, early 2012, and he enrolled at Phoenix College in January 2012. As part of the application and enrollment process, Mr. Liebich provided personally identifiable information including but not limited to his name, address, phone number, email address, Social Security Number, date of birth, certain demographical information, and enrollment, academic, and financial aid information.

55. Phoenix College requested this information from Mr. Liebich as a condition of his application and enrollment. Mr. Liebich provided the information understanding that Phoenix College would safeguard his information from unauthorized disclosure. Mr. Liebich understood and expected that Phoenix College maintained the security of its

data systems in accordance with MCCCD policies, industry standards, and state and federal law.

56. Mr. Liebich heard about the data breach in early 2014 but did not receive notice of the breach from MCCCD directly. While MCCCD had mailed notice of the data breach to some former and current students, employees, and vendors, MCCCD had not mailed notice of the data breach to Mr. Liebich.

57. Mr. Liebich called MCCCD to verify whether his PII was included in the data breach.

58. MCCCD informed Mr. Liebich that his personal information was included in the data breach and that MCCCD would send him a letter notifying him of the breach.

59. MCCCD failed to send Mr. Liebich the requested letter. Mr. Liebich is in the process of requesting a copy of the letter again.

60. The letter MCCCD sent out to data breach victims stated that MCCCD "recently discovered" that MCCCD "IT systems may have been accessed without authorization."

61. The letter advised that "on October 18th, 2013, we determined that your information, including your name, address, phone number, e-mail address, Social Security number, date of birth, certain demographical information, and enrollment, academic and financial aid information may have been accessed without authorization."

62. The letter claimed that "immediately" after discovering the breach, MCCCD conducted an investigation and took steps to enhance security measures to "prevent this type of event from happening again."

63. The letter stated that MCCCD was "not aware of any misuse of your information" but "out of an abundance of caution" MCCCD hired Kroll to provide one year of its "ID TheftSmart program," which includes "Continuous Credit Monitoring and Enhanced Identity Theft Consultation and Restoration."

64. The letter then provides instructions to on how to receive the Kroll services.

65. Mr. Liebich has not been able to take advantage of that credit monitoring because MCCCD has failed to provide him with a copy of this letter and those instructions.

66. Mr. Liebich has requested credit reports from the major credit reporting agencies. Mr. Liebich had to bear the cost of obtaining these reports, an expense of approximately ten dollars per month, paid out of pocket.

67. Mr. Liebich is continually monitoring his bank accounts and credit cards for any unauthorized or suspicious activity.

68. In 2013, Mr. Liebich discovered fraudulent charges on his debit card. Although he does not how his bank account information was procured, it could have been obtained as a result of the MCCCD breach.

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

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

70. Cyber criminals would not have access to MCCCD's network but for MCCCD's inadequate security protections and willful failure to act once those inadequacies were identified. MCCCD failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information that was compromised.

71. Despite the risk posed to current and former students, employees, and vendors, MCCCD did not immediately notify the affected individuals of the breach. Additionally, in its letter sent to some (but not all) of the 2.5 million affected individuals, MCCCD also claimed that it "recently discovered" the breach and "[i]mmediately after learning of this situation, we initiated a thorough investigation," "and implemented measures designed to prevent this type of event from happening again." MCCCD also downplayed the threat to the affected individuals by assuring that "we are not aware of

any misuse of your information" and that that it was providing credit monitoring "out of an abundance of caution."

72. These claims by MCCCD imparted a false sense of security to affected individuals and misrepresented the facts. In reality, MCCCD had failed to investigate and remedy known data breach problems over a period of three years, MCCCD had waited seven months after the latest breach to provide notice, and MCCCD's offer of short-term credit monitoring by a company of MCCCD's choosing was an insufficient remedy.

73. MCCCD's failure to promptly and effectively inform students, employees, and vendors earlier of the data theft left an untold number vulnerable to attack.

74. As a result of MCCCD's unfair, inadequate, and unreasonable data security, cyber-criminals claimed the ability to sell the personal information of Plaintiff and the Class and, in the case of employees, their financial information as well. As a result, breach victims must add themselves to credit fraud watch lists, which substantially impair the victims' ability to obtain additional credit. Because names, addresses, phone number and email addresses were stolen and made available for sale, there is a real and compounding risk that Plaintiff and the Class will be victims of identity theft.

75. Immediate notice of the breach is essential to obtain the best protection afforded by identity theft protection services. MCCCD failed to provide such immediate notice, thus further exacerbating the damages sustained by Plaintiff and the Class resulting from the breach.

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

77. The PII that MCCCD failed to adequately protect, including Plaintiff's identifying information, is "as good as gold" to identity thieves because identity thieves can use victims' personal data to open new financial accounts and incur charges in

another person's name, take out loans in another person's name, incur charges on existing accounts, or clone ATM, debit, or credit cards.

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

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

80. Although MCCCD ultimately offered free credit monitoring, the credit monitoring services will not prevent identity theft or protect Plaintiff and the Class for more than a year. Meanwhile, personal information could be misused by identity thieves and others years into the future.

81. Moreover, experts warn that when a breach occurs "[o]ne year of credit monitoring may not be enough. Hackers tend to lay low when data breaches are exposed...They often wait until consumers are less likely to be on the lookout for fraudulent activities."[3] Thus, Plaintiff and the Class must take additional steps to protect their credit and identities.

---

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

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

[3] http://online.wsj.com/news/articles/SB10001424052702304856504579337263720948556.

82. In fact, the FTC recommends placing an extended fraud alert with each credit reporting agency after your identity has been compromised.[4] These fraud alerts last for seven years.

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

84. And, according to a 2011 report by Javelin Strategy and Research, individuals who receive a data breach notification letter are more than four times as likely to become victims of identity theft, average out-of-pocket costs to remedy a data breach are $631, and data breach victims spend an average of 41 hours resolving the breach.[5]

IV. CLASS ALLEGATIONS

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

> All persons and entities whose Personally Identifiable Information existed or was being maintained on MCCCD electronic data systems on or before November 27, 2013.

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

87. ***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

---

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

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

determined at this time, 2.5 million persons and entities had their Personally Identifiable Information compromised in the data breach that MCCCD first disclosed on November 27, 2013.

88. ***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 MCCCD implemented reasonable and industry-standard safety measures to protect Class members' Personally Identifiably Information;

b. whether MCCCD knew or should have known that its ITS system was not secure;

c. whether MCCCD failed to secure its ITS system once MCCCD determined those systems had been breached;

d. whether MCCCD was negligent in adopting, designing, implementing, or supervising its ITS security systems, in failing to remedy any breach of its ITS systems, and in failing to timely notify Plaintiff and the Class that their Personally Identifiable Information had been breached;

e. whether MCCCD breached its express or implied contractual duties to Plaintiff and the Class by failing to implement its Best Practices and Reasonable Protection policy; and

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

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

90. ***Adequacy***. Plaintiff and his counsel will fairly and adequately represent the interests of the Class members. Plaintiff has no interests antagonistic to, or in conflict

with, the interests of the other class members, and he will zealously pursue the claims in this action. Plaintiff's lawyers are highly experienced in the prosecution of consumer class actions and complex commercial litigation, capable of providing the financial resources necessary to litigate this matter to conclusion, and have litigated other data breach matters in a class context.

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

92. 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.

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

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

V. CLAIMS FOR RELIEF

CLAIM I

Negligence

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

96. By requesting and accepting Plaintiff's and Class members' Personally Identifiable Information, MCCCD assumed a duty requiring it to use reasonable and industry standard care to secure such information against theft and misuse.

97. MCCCD breached its duty of care by failing to adequately secure and protect Plaintiff's and the Class members' Personally Identifiable Information from theft, collection, and misuse by third parties.

98. Once MCCCD became aware that Plaintiff's and the Class' Personally Identifiable Information was for sale on the internet and was subject to a security breach, MCCCD acted with reckless indifference and conscious disregard of Plaintiff's and the Class members' rights by failing to take any remedial action to protect their Personally Identifiable Information. MCCCD's actions (or inactions) created a substantial and unjustifiable risk of serious harm to Plaintiff and the Class.

99. MCCCD further breached its duty of care by failing to promptly, clearly, accurately, and completely inform Plaintiff and the Class that their Personally Identifiable Information had been breached.

100. Among other things, MCCCD's failure to safeguard Plaintiff's and Class members' Personally Identifiable Information, and the resulting data breach, has left Plaintiff and class members exposed to greatly increased, long-term risk of identity theft, including without limitation well-known risks of credit damage, reputational harm, and financial loss.

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

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

103. As a direct and proximate result of MCCCD's failure to take reasonable care and use industry standard measures to protect the Personally Identifiable Information placed in its care, Plaintiff's and Class members' Personally Identifiable Information was disclosed or acquired by unauthorized parties, to the detriment of each class member.

104. As a direct and proximate result of MCCCD's negligence and misconduct, Plaintiff and the Class were injured in fact by the unauthorized disclosure of their Personally Identifiable Information, and are entitled to recover the costs associated with the detection and prevention of identity theft, including credit monitoring, identity theft consultation, and identity restoration, and with the detection and prevention of unauthorized use of their financial accounts, including credit monitoring, all of which have an ascertainable monetary value to be proven at trial.

105. As a direct and proximate result of MCCCD's reckless indifference and conscious disregard for Plaintiff's and the Class members' rights, Plaintiff and the Class are also entitled to punitive damages.

CLAIM II

Breach of Contract, Express and Implied

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

107. As a condition of application, enrollment, employment, and business contracts, MCCCD requested Plaintiff's and Class members' Personally Identifiable Information. Plaintiff and Class members provided Personally Identifiable Information to MCCCD in accordance with MCCCD's contractual requirements.

108. MCCCD, through its Best Practices and Reasonable Protection policy, promised to protect this information and take reasonable measures to ensure its security. MCCCD's Best Practices and Reasonable Protection policy is incorporated into MCCCD's contracts with Plaintiff and the Class.

109. To the extent that MCCCD's contracts allow discretion on how to implement its Best Practices and Reasonable Protection policies, MCCCD exercised that discretion in bad faith.

110. MCCCD breached its express and implied contractual duties when it failed to establish "appropriate and reasonable safeguards" to protect and "restrict access" to Plaintiff's and the Class members' Personally Identifiable Information.

111. MCCCD further breached its express and implied contractual duties with Plaintiff and the Class when MCCCD discovered that Plaintiff's and Class members' Personally Identifiable Information had been breached and, nevertheless, failed to act in accordance with MCCCD's own protocols to remedy the breach or mitigate any damages to Plaintiff and the Class.

112. Among other things, MCCCD's failure to safeguard Plaintiff's and Class members' Personally Identifiable Information, and the resulting data breach, has left Plaintiff and class members exposed to greatly increased risk of identity theft, including without limitation well-known risks of credit damage, reputational harm, and financial loss.

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

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

115. As a natural and probable consequence of MCCCD's breach of contract, Plaintiff's and Class members' Personally Identifiable Information was disclosed to unauthorized parties, to the detriment of each class member.

116. Because of MCCCD's breach of contract, Plaintiff and the Class were injured in fact by the unauthorized disclosure of their Personally Identifiable Information, and are entitled to recover all costs associated with the detection and prevention of

identity theft, including credit monitoring, identity theft consultation, and identity restoration, and with the detection and prevention of unauthorized use of their financial accounts, all of which have an ascertainable monetary value to be proven at trial.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff respectfully requests the following relief:

A. That the Court certify this case as a class action and appoint Plaintiff Jason Liebich to be Class Representative and Hagens Berman Sobol Shapiro, LLP, as Class Counsel;

B. That the Court certify Claim I under Ariz. R. Civ. P. 23(b)(3);

C. That the Court certify Claim II under Ariz. R. Civ. P. 23(b)(2);

D. That the Court award Plaintiff appropriate compensatory damages, including without limitation damages associated with credit monitoring, credit restoration, and identity protection, as well as punitive damages,

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

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

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

JURY TRIAL DEMANDED

Plaintiff demands a trial by jury on all issues.

DATED this 15th day of April, 2014.

Respectfully submitted,

HAGENS BERMAN SOBOL SHAPIRO LLP

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

GRANT WOODS P.C.
J. Grant Woods (006106)
Two Renaissance Square
40 N. Central Avenue, Suite 2250
Phoenix, AZ 85004
Telephone: (602) 258-2599
Facsimile: (602) 258-5070
E-mail: gw@grantwoodspc.net

Attorneys for Plaintiff