Paul L. Stoller (Bar No. 016773)
Mark A. Fuller (Bar No. 012149)
Jeffrey T. Pyburn (Bar No. 011050)
Kiersten A. Murphy (Bar No. 022612)
Christopher W. Thompson (Bar No. 026384)
GALLAGHER & KENNEDY, P.A.
2575 East Camelback Road
Phoenix, Arizona 85016-9225
Telephone: (602) 530-8000
Facsimile: (602) 530-8500
E-mails: paul.stoller@gknet.com
mark.fuller@gknet.com
jtp@gknet.com
kam@gknet.com
chris.thompson@gknet.com

Attorneys for Plaintiffs

SUPERIOR COURT OF THE STATE OF ARIZONA

COUNTY OF MARICOPA

CHADRICK ROBERTS, an individual, and MARK McKEE, an individual, on behalf of themselves and all similarly-situated persons and entities;

Plaintiffs,

v.

THE MARICOPA COUNTY COMMUNITY COLLEGE DISTRICT, a political subdivision of the State of Arizona,

Defendant.

No. CV2014-007411

CLASS ACTION COMPLAINT

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

1. This is a class action lawsuit brought on behalf of Plaintiffs and all other persons similarly situated against The Maricopa County Community College District ("the District") for its failure to adequately protect the confidential, private personal information of its current and former students and applicants, parents of students and applicants, employees, vendors, and other individuals and businesses.

2. The personal identifying information ("PII") provided to the District by Plaintiffs and other class members, to be held in the strictest confidence, includes names, addresses, phone numbers, e-mail addresses, Social Security numbers, dates of birth, demographic information, and as-yet-unidentified "enrollment, academic and financial aid information." The District has collected and stored all of this information for decades.

3. The Federal Bureau of Investigation notified the District in April 2013 that the District's databases containing the PII of Plaintiffs and other class members was for sale on the Internet. As a practical matter, such a disastrous data breach had been inevitable. For years, the District had known of the vulnerabilities in its electronic information technology systems and databases, had known of the substantial risk of public disclosure and exploitation of that PII, and had negligently, recklessly and/or knowingly failed to take appropriate steps to remediate those vulnerabilities.

4. Having exposed and compromised the PII of Plaintiffs and other class members, the District chose not to notify the victims, and instead undertook "remediation" which, upon information and belief, destroyed the evidence as to what data actually made its way into the hands of others. It was not until November 2013 – seven months after learning of the breach – that the District even began notifying victims, and it did so through a form letter in which it deliberately misled and deceived them about what had happened and the true nature of the risks posed to Plaintiffs and the other class members.

5. As a result of this and other misconduct by the District, described in greater detail below, Plaintiffs and other class members have suffered great harm. Unlike a credit card number, the PII exposed in this matter is tantamount to a gift-wrapped package for anyone seeking to steal someone's identity. Some class members have already suffered identity theft, and all class members will remain at serious risk of identity theft far into the future. There is no way to put the genie back in the bottle.

6. Plaintiffs therefore bring this action seeking redress and compensation for the harm caused to them and the other class members by virtue of the District's conduct.

PARTIES, JURISDICTION AND VENUE

7. Plaintiff Chadrick Roberts is a resident of Maricopa County, Arizona. Mr. Roberts served the District with a Notice of Claim on January 2, 2014. The District denied the notice by failing to respond by the statutory deadline in A.R.S. § 12-821.01.

8. Plaintiff Mark McKee is a permanent resident of Maricopa County, Arizona, now resident in New York. Mr. McKee served the District with a Notice of Claim on January 30, 2014. The District denied the notice by failing to respond by the statutory deadline in A.R.S. § 12-821.01.

9. The District is a political subdivision of the State of Arizona operating in Maricopa County, Arizona.

10. The Court has jurisdiction pursuant to A.R.S. § 12-123, and venue is proper in this Court pursuant to A.R.S. § 12-401.

FACTS

11. The District operates ten colleges, two skill centers, and a number of other educational centers in Maricopa County.

12. For years, the District has collected PII from applicants, students and employees, their family members, and vendors. The District has described the PII as including "names, addresses, phone numbers, e-mail addresses, Social Security numbers, dates of birth, demographic information," as well as unspecified "enrollment, academic and financial aid information."

13. More specifically, upon information and belief, the PII includes names, addresses, dates of birth, Social Security numbers, motor vehicle registration, driver's license information, bank account information (including routing numbers and checking account numbers), financial investment information, criminal background information, "limited benefits" information, telephone numbers, email addresses, Veterans Affairs file numbers, birth certificate information, passport information, State identification card information, military identification card information, Tribal identification card information, naturalization card information, alien registration card information, prior

school transcripts with a photograph, information from certificates of naturalization and/or citizenship, information from Tribal certificates of Indian Blood and Bureau of Indian Affairs affidavits of birth, tax identification information, voter registration information, employment history information, financial support information, and location and ownership of real property assets.

14. In collecting PII, the District explicitly and implicitly promises, represents and warrants that it will respect and ensure the privacy and confidentiality of that information. For example, in its applications for enrollment or employment the District states:

- "Your SSN will not be used as your primary student identification number and will be kept confidential" (emphasis in original);
- "**ALL OF THE INFORMATION ON THIS FORM IS CONFIDENTIAL AND IN COMPLIANCE WITH THE FAMILY EDUCATION RIGHTS AND PRIVACY ACT**" (emphasis in original);
- "Your Social Security Number will not be used as your primary student identification number and will be kept confidential."
- Students should be aware that a correct Social Security Number must be on file for reporting information pertaining to potential tax credit, and must be used by applicants for federal and state aid, and Veteran Administration benefits. Failure to provide a correct Social Security Number may preclude the determination of eligibility for in-state residence . . . ."; and
- "All Motor Vehicle Record and Driving History reports are confidential and will be disclosed as appropriate only to those MCCCD employees with a legitimate reason to know, such as College Safety Directors, Legal Services, Human Resources, and supervisors."

15. Likewise, the District publicly acknowledges "its affirmative duty and continuing need to protect confidential employee and student data and to maintain the confidentiality of that data." Internally, in its Data Access and Appropriate Use Best

Practices Document, the District recognizes that this requires implementing appropriate and reasonable administrative, technical, and physical safeguards to "ensure the security and protection of confidential information in its custody," to "protect against any anticipated threats of hazards to the security and integrity of such confidential information," and to "protect against unauthorized access to or use of such confidential information."

16. The District also represents and warrants that it is complying with its obligations under relevant state and federal legislation, including the Federal Education Rights Privacy Act ("FERPA"), the Health Insurance Portability and Accountability Act ("HIPAA"), the Gramm-Leach-Bliley Act ("GLBA"), Federal Trade Commission ("FTC") Regulations (16 CFR, Part 314), Standards for Safeguarding Consumer Information, and A.R.S. § 15-141. As the District has acknowledged, this includes, for example, a duty under the GLBA to "detect, prevent and respond to attacks, intrusions, or other system failures," and duties under FTC regulations to: (a) "identify reasonably foreseeable internal and external risks to the security, confidentiality and integrity of consumer information that could result in the unauthorized disclosure, misuse . . . or other compromise of such information"; (b) "design and implement safeguards to control the risks [it] idenitif[ies] through risk assessment, and regularly test or otherwise monitor the effectiveness of safeguards . . . "; and (c) "evaluate and adjust [its] information security program in light of the results of the testing and monitoring required [by these provisions] . . . ."

17. Notwithstanding its representations, promises, and duties to protect and to safeguard the PII it collects and stores, the District has for years failed to do so, leading ultimately to a massive breach and disclosure which upon information and belief was discovered by the Federal Bureau of Investigation in 2013.

18. To date, the District has hidden the truth about the events concerning this breach, and has affirmatively misled the public about those events. Even without the benefit of full, honest disclosure, however, Plaintiffs are aware of facts showing that the

District acted with reckless disregard of its duties and the welfare of the persons whose PII was at risk, knowingly and intentionally failing to address and to remedy what it knew were serious vulnerabilities in its IT systems and databases. Such facts include those alleged in the following paragraphs, many of which are taken from a chronology prepared by a third party after reviewing District documents and interviewing District IT department whistleblowers. The chronology was provided to the District's Board in a public meeting, along with dozens of supporting documents, and is publicly available on the internet (although the District removed it as an attachment to the minutes of the meeting).

19. In January 2011, more than two years before learning of the breach in 2013, the District learned that one or more of its databases were available for sale on the internet ("the 2011 Breach"). The District learned that its databases and webservers had been compromised, allowing root and shell access to third parties on multiple occasions. As reported widely in the media, the third parties involved were identity thieves who exploited commonly known security vulnerabilities in institutions' webservers and databases, and were selling access to the PII they had illegally obtained.

20. Upon information and belief, within days of first learning of the 2011 Breach, District IT employees provided reports on the scope and severity of the security and vulnerability issues that were plaguing the District's network servers and databases. These reports were given to District Vice-Chancellor George Kahkedjian and other IT Division leaders.

21. On January 25, 2011, Vice-Chancellor Kahkedjian made a presentation to the District's Governing Board concerning the 2004 GO Bond IT funding allocations, and nominated "Network and Network Security" as a key area of MCCCD's District-Wide Strategic Plan. The minutes of these meetings, however, do not reflect that Kahkedjian or anyone else disclosed the 2011 Breach to the Board, or that the District's webservers were currently known to be unsecure and accessible to unauthorized access through the internet.

22. By January 30, 2011, the root cause for the webserver compromise was identified by District IT employees and outside consultants Stach & Liu (now known as Bishop Fox). These IT employees outlined extensive action items, including the need for further investigations and remediation plans to address and fix the widespread security flaws. Upon information and belief, these action items were circulated to District superiors, including Vice-Chancellor Kahkedjian.

23. IT employees and the Stach & Liu consultants continued to investigate the security status of the District's databases and webservers. These investigations led to numerous reports outlining further systemic security concerns of District-wide information systems technologies.

24. The results of the investigation painted a dire picture. There were substantial security flaws throughout the District's networks, including active communications between the District's webservers and external hosts that had existed for months. Moreover, the District lacked the ability to conduct in-depth monitoring of its systems for these instructions, could not routinely scan for vulnerabilities, had no formal emergency response protocol, and could not determine the risks to data at its ten college campuses throughout Maricopa County.

25. By the end of February 2011, the District had still not taken any corrective action to address the known security vulnerabilities, and its compromised webservers and databases were still not secure. Nor had the District notified those at risk for exploitation of their PII.

26. In March 2011, Vice-Chancellor Kahkedjian sent a District-wide email regarding what he called "an information security issue that came up recently." In it, he disclosed that "an internet site had announced that the personnel data of a number of education institutions, including [MCCCD], was for sale," but stated that "[t]he site was shut down before we could verify this claim." He also reassured the readers by stating that the District "promptly investigated to see if any breaches of privacy data or personal information occurred. To date, we have found no such breaches." What the Vice-

Chancellor carefully chose not to divulge, however, was that the District had learned of the security breaches from the FBI, which had informed the District that PII was in fact available for purchase on the internet. Moreover, the Vice-Chancellor failed to mention the fact that he had been informed by IT employees that the District's electronic information systems had been contacted through external hosts on the internet numerous times, possibly hundreds.

27. In the same email, the Vice-Chancellor told readers that the District was "taking steps to create a more secure web environment, including stronger network and security access." In fact, however, over the course of the next eight months, District IT employees tried unsuccessfully to have District senior administration address and remedy the ongoing security vulnerabilities and compromised webservers.

28. Upon information and belief, in the spring of 2011, the District's outside consultants Stach & Liu submitted a report on their own internal investigation into the 2011 Breach. Upon information and belief, the Stach & Liu report described the extent of the breach, and identified the existing problems that needed to be mitigated. Upon information and belief, Stach & Liu provided the report to District IT employees, who in turn provided the report to Vice-Chancellor Kahkedjian. But neither the Vice-Chancellor nor any other District Senior Administrator took any of the actions recommended in the Stach & Liu report. Nor did they take any other reasonable and appropriate action to remediate the problems outlined in the report.

29. Meanwhile, the Vice-Chancellor attended a Working Session of the District's Governing Board, where he presented on the "Systemic Approach to Information Technology." The minutes of this meeting reflect the Vice-Chancellor's acknowledgment that the "major role of IT governance is to outline the decision rights and accountability framework to encourage desirable behavior in using IT." He further represented that a newly formed Information Technology Leadership Council ("ITLC") would create and implement full district-wide standards by June 30, 2011 that would lead to "increased and simplified security."

30. On or about June 30, 2011, the Auditor General's Office of the State of Arizona began compiling its audit of the District's internal control and compliance for the Year Ended June 30, 2011. Upon information and belief, District leadership failed to inform the Auditor General's Office of the 2011 Breach during its audit.

31. At the same time, District employees continued to hold meetings with District leadership, warning that the compromised webservers were still in operation and "possible corruptions to other systems" within District posed addition security risks.

32. By mid-November 2011, the webserver and other security issues were still not resolved. By this time, however, some District employees were finally running network scans to test the District's systems for vulnerabilities. In a November 16, 2011, email, District employee Joyce McQueen alerted her supervisor Rod Marten that the scans had identified over 200 vulnerabilities.

33. Mr. Marten dismissed the scan results as "not equivalent to 'vulnerabilities.'" In fact, as Mrs. McQueen explained to him, "the word 'vulnerability' [was not her] interpretation, [but] exactly what the [security software] stated."

34. The District took no action to address the issues raised in Mrs. McQueen's report. The compromised webservers remained in operation, and the numerous reported system vulnerabilities remained unremediated. To try and spur the District and its senior leadership to address those issues, District IT employees delivered an Oversight Report to Vice-Chancellor Kahkedjian.

35. The Oversight Report detailed two of the most pressing and specific risks to the security of the District's systems containing PII. First, the webservers compromised in 2011 had still not been fixed, were still in operation, and were still accessible in the same manner that allowed the 2011 Breach. Second, the security systems that were supposed to monitor the network and servers throughout the District were not operational. The Oversight Report, noted that "[a]fter 9-10 months, none of the agreed upon next steps have been accomplished. We are still running on a compromised

server . . . . The risk to MCCCD of running a compromised server is very high. The potential impact is critical."

36. Shortly after the Oversight Report was prepared, the Auditor General issued findings and conclusions from its audit of the District's computer access and change controls. The November 27, 2011, Report noted that the District needed to strengthen "computer access and modification controls" and noted a number of deficiencies in the District's monitoring of access to its computerized systems. The findings were "similar to a prior-year finding."

37. On December 16, 2011, the District responded to the Auditor General's findings. With respect to the need to strengthen computer access and change controls, the District stated that it "agrees with the findings and will address the issues identified." The District also represented that it anticipated completing the necessary work by February 2012.

38. On March 6, 2012, Vice-Chancellor Kahkedjian provided the Governing Board with an "Update on Information Technology Strategic Plan & Governance." He stated that the District was "consistent with the industry regarding technology controls, managerial and operational controls," and that "security has been worked with very carefully." Weeks later, however, District employees were still informing the Vice-Chancellor of the substantial, severe, and ongoing security problems and risks resulting from the District's failure to address the compromised webservers and other vulnerabilities that should have been fixed immediately after discovering the 2011 Breach.

39. The Vice-Chancellor continued to ignore all the warnings, and began to retaliate against IT employees who were voicing their concerns. At a July 23, 2012 Governing Board meeting, Linda Brown, founder of the Maricopa Citizens for Safety and Accountability, requested the Governing Board to order an independent investigation of the District IT department. At an August 28, 2012 Governing Board meeting, the President of the Management, Administration and Technology employee group ("MAT")

Executive Council and the District-wide Professional Staff Association ("PSA") President delivered public messages explaining that they had been contacted by "several employees in the Information Technology Services division with complains of maltreatment, intimidation, retaliation, and outright abuse at the hands of management, particularly in regard to ITS reorganization." The President of MAT and the PSA President both requested "that an independent external evaluator be brought in to objectively assess the situation in IT, determine the legitimacy of the employee allegations, and recommend steps for improvement."

40. The District took no constructive action in response to these requests. It certainly did nothing to cure the security issues that continued to plague its electronic information systems.

41. In a subsequent Grievance filed with the District, IT employees noted the security and operational problems that had become systemic in the District's IT department. The Grievance reminded the Chancellor that the prior Oversight Report had "pointed out several risks and deficiencies in the organization" and that "most of the recommendations were ignored . . . includ[ing]: Resolution of the web server compromises," which "represented a high risk to the organization that could expose personal information." The Grievance also reminded the Chancellor that the prior Oversight Report had "pointed out several risks and deficiencies in the organization" and that "most of the recommendations were ignored . . . includ[ing]: Resolution of the web server compromises," which "represented a high risk to the organization that could expose personal information." But, the District did nothing.

42. On November 27, 2012, the Auditor General released its Report on Internal Control and Compliance for the District, for the Year Ended June 30, 2012. This Report paralleled the 2011 Report, finding that "the District did not adequately limit logical access to its information systems during the year," and "there is an increased risk that unauthorized access to the District's systems, including financial information and data that is confidential or sensitive in nature, may not be prevented or detected." On

January 10, 2013, the District again responded by stating that "[t]he District agrees with the finding and recommendation." In a public meeting, a representative of the Vice-Chancellor stated that for the District, "data is a critical issue and it is priceless."

43. Still the District did nothing. By the spring of 2013, it had known for more than two years about systemic and wide-ranging security concerns with District-wide electronic information systems technology. Time and again District employees raised the alarm, warning those in charge that the security threats had not been fixed, that the District had failed to follow through and to implement the necessary steps to protect the data, that the databases and webservers were still compromised and vulnerable to intrusion, and that the situation posed financial risks to the District and imperiled the confidential PII of students, parents, faculty, employees, and vendors. The District not only turned a blind eye to the problems, but ultimately attacked those who had the courage to voice their concerns.

44. What followed was inevitable. In April 2013, the FBI alerted the District – again – that PII collected by the District was available for purchase on the Internet. This 2013 breach (the "2013 Breach") resulted from the same vulnerabilities that had been exploited in 2011, and involved fourteen or more databases.

45. Notwithstanding the obvious threat of identity theft posed by this revelation, the District chose not to disclose the data breach to the public for approximately seven months, during which time it hired legal counsel and undertook an investigation of some kind. Although the District has yet to divulge any details of what it did during this long delay before notifying those affected by the breach, its counsel eventually disclosed to at least one state's Attorney General that, in the course of "responding" to the 2013 Breach, the District destroyed the evidence as to what and whose PII was actually taken.

46. Before notifying the victims, and at the request of the Chancellor, the District's Governing Board approved an update to its Governance Manual. Previously, and throughout the period since the 2011 Breach, section 2.5 of the Manual had provided, among other things, that "[w]ith respect to Identity Theft Red Flag and Security Incident

Reporting, the Chancellor shall not operate without implementing a program to assist individuals in detecting, preventing, and mitigating identity theft, and to provide information for the reporting of a security incident." It had also provided that "[t]he Chancellor may not make changes to the Identity Theft Red Flag and Security Incident Reporting policy without prior notification to the Board. On October 22, 2013 the Board removed this and other restrictions, replacing them with a vague statement that "[t]he Chancellor shall not cause or allow institutional assets to be unprotected, inadequately maintained, or unnecessarily risked."

47. In early December 2013, the Auditor General released its 2013 Report, which disclosed, among other things, that "in April 2013, the District's network security was breached by hackers resulting estimated costs of 16.8 million to remedy vulnerabilities within its information systems and to provide credit monitoring to an estimated 2.6 million individuals." A few weeks earlier, recognizing that release of the Report was imminent, the District approved a three-year extension to Chancellor Glasper's employment, and then, the next day, began notifying victims of the 2013 Breach by way of a form letter designed to minimize the threat and provide a false sense of comfort.

48. In its form notice letter, which was supposedly sent to approximately 2.5 million people beginning on or about November 27, 2013, the District advises that there was an "incident" which "may" have resulted in what the District calls "unauthorized access" to the confidential information described above. Without mentioning the 2011 data breach, let alone the District's failure to institute appropriate security measures in the aftermath of that breach, the letter tells recipients that "we take the security of your personal information very seriously." The District's form notice letter goes on to reassure the recipients that "we are not aware" of "misuse" of the information – neglecting to mention that the databases were available for sale on the Internet (a second time), and that the District has no basis to say that any victim's data was not, or will not be, misused.

49. As if all of this were not misleading enough, the District's form notice letter reassures victims that the systems accessed "did not contain credit card information or personal health information," as if they need not be concerned. In fact, the data breach is *vastly* more serious than the disclosure of credit card information. Credit cards are easily canceled, and issuers have fraud detection systems in place which alert consumers about suspicious activity and place holds on cards. And consumers typically do not pay for unauthorized charges. In contrast, the PII exposed in this matter is tantamount to a gift-wrapped package for anyone seeking to steal someone's identity, and the threat will follow each person for the rest or his or her life.

50. The District's letter to victims offers a kind of Band-Aid, stating that the District will provide "identity safeguards and other services at no cost to you for one year through [Kroll's] ID TheftSmart program." This "offer," which has become a customary ploy to stave off claims, provides scant protection and is woefully insufficient to address the harm suffered by the victims of the District's conduct.

51. As a threshold matter, the monitoring offer comes far too late. The District did not even begin notifying victims until more than seven months after the 2013 Breach, and even now, upon information and belief, some victims still have yet to receive the letter. The offer also requires affirmative action by the victims, the vast majority of whom the District knows are not likely to receive the notice or to sign up. In fact, as the press has reported, many recipients viewed the form letter itself as a scam. Meanwhile, the "monitoring" is less than comprehensive, and one year is wholly inadequate for victims whose compromised PII includes an entire package of information including Social Security numbers and dates of birth.

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

53. Neither Plaintiffs nor the members of the class authorized the District to disclose their PII to the public.

54. The District's actions, including its knowing failure to implement the necessary steps to protect that PII, has resulted in attempted and actual identity theft for many members of the class and has exposed the remaining members of the class to the potential for such identity theft for the remainders of their natural lives.

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

PLAINTIFFS AND OTHER CLAIMANTS

56. Plaintiff Chad Roberts is a former student in the District. As such, he provided his PII to the District, which would have included, among other things, his date of birth, name, address, Social Security number, current and former addresses, telephone numbers, email addresses, marital status, motor vehicle records information, place of employment, and financial information.

57. Mr. Roberts received the District's form notice of the 2013 Breach as described above, and is one of approximately 2.5 million victims of the breach. He has suffered substantial, irreparable harm by virtue of the fact that his PII was compromised and disclosed to one or more criminals whose identity remains unknown, and that his PII will remain at risk, in the public domain, permanently.

58. Mr. McKee is a former student at Brophy College Preparatory who, like many Brophy students, was dual-enrolled in the District. As such, he provided his PII to the District, which would have included, among other things, his date of birth, name, address, Social Security number, current and former addresses, telephone numbers, email

addresses, marital status, motor vehicle records information, place of employment, and financial information.

59. Mr. McKee received the District's form notice of the 2013 Breach as described above, and is one of approximately 2.5 million victims of the breach. He has suffered substantial, irreparable harm by virtue of the fact that his PII was compromised and disclosed to one or more criminals whose identity remains unknown, and that his PII will remain at risk, in the public domain, permanently.

60. Other victims of the 2013 Breach have *already* suffered identity theft as a result of the 2013 Breach, some of whom have served Notices of Claim on the District. These claimants' experiences confirm that the PII available on the internet was in fact misappropriated, has in fact been misused, and will in fact be misused in the future.

61. For example, Rebecca Barber, Ph.D., has been an adjunct faculty member in the District for a number of years. As such, she provided her PII to the District, which would have included, among other things, her date of birth, name, address, Social Security number, current and former addresses, telephone numbers, email addresses, marital status, motor vehicle records information, place of employment, and financial information. Dr. Barber is a victim of the 2013 Breach, and submitted a Notice of Claim to the District on March 25, 2014.

62. In her Notice of Claim, Dr. Barber explains that she is a victim of identity theft as a result of the District's conduct. Although she is very sensitive to the potential for identity theft, and takes great care to protect the secrecy of her PII, a thief with access to her PII recently opened a BillMeLater credit account in her name, using, among other things, her full name, address, date of birth, and Social Security Number.

63. Dr. Barber is vigilant in protecting her PII, takes reasonable precautions to keep it out of the public domain, and is unaware of any other breach or theft that could have been the source of one or more identity thieves obtaining her PII. Under the circumstances, the overwhelming inference is that the identity theft was a direct and proximate result of the 2013 Breach.

64. Notwithstanding Dr. Barber's efforts to respond to the theft (for example, filing reports with the police and FTC and putting fraud alerts on her credit), there is nothing she can do about the fact that her PII was disclosed to one or more criminals whose identity remains unknown, and that her PII will remain at risk, in the public domain, permanently.

65. Dr. Barber's experience also illustrates the inadequacy of the District's proposed "remedy" to the data breach, and the misleading nature of the District's form notice to the victims. Relying on the assurances and instructions in that letter, Dr. Barber subscribed to the free one-year offer with Kroll, only to learn later that Kroll's "services" did not catch the BillMeLater identity-theft incident. Although she was a Kroll subscriber at the time the BillMeLater fraud occurred, Kroll did not alert her to the fraud, and instead notified Dr. Barber that there had been no activity on her credit report, well after she had been alerted to the identity theft and fraud by BillMeLater.

66. Emily Gibbs is another former student in the District. As such, she provided her PII to the District, which would have included, among other things, her date of birth, name, address, social security number, current and former addresses, telephone numbers, email addresses, marital status, motor vehicle records information, place of employment, and financial information. Ms. Gibbs is a victim of the 2013 Breach, and submitted a Notice of Claim to the District on April 11, 2014.

67. In her Notice of Claim, Ms. Gibbs explains that she is a victim of identity theft as a result of the District's conduct. Specifically, one or more thieves with access to her PII opened a series of fraudulent credit card accounts in her name, made purchases around the country, and even obtained $10,000 in financing from a bank which was used to pay for medical services.

68. Ms. Gibbs is vigilant in protecting her PII, takes reasonable precautions to keep it out of the public domain, and is unaware of any other breach or theft that could have been the source of one or more identity thieves obtaining her PII. Under the

circumstances, the overwhelming inference is that the identity theft was a direct and proximate result of the 2013 Breach.

69. Notwithstanding Ms. Gibbs's efforts to respond to the situation (for example, filing a police report, dealing with the lenders involved, and placing a fraud alert with Experian), there is nothing she can do about the fact that her PII was disclosed to one or more criminals whose identity remains unknown, and that her PII will remain at risk, in the public domain, permanently.

70. Gary Vigneault, a law enforcement officer with more than thirty years' experience, is a former student within the District, and has been employed as an instructor within the District for many years as well. As such, he provided his PII to the District, which would have included, among other things, his date of birth, name, address, social security number, current and former addresses, telephone numbers, email addresses, marital status, motor vehicle records information, place of employment, and financial information. Officer Vigneault is a victim of the 2013 Breach, and submitted a Notice of Claim to the District on April 11, 2014.

71. In his Notice of Claim, Officer Vigneault explains that he is a victim of identity theft as a result of the District's conduct. Specifically, one or more thieves with access to his PII filed a fraudulent tax return in his name, which only came to his attention when he filed attempted to file his own return before the April 15, 2014 deadline. In addition, Officer Vigneault was alerted that one or more thieves have attempted unauthorized access to mortgage information on residential property he owns.

72. Officer Vigneault is vigilant in protecting his PII, takes reasonable precautions to keep it out of the public domain, and is unaware of any other breach or theft that could have been the source of one or more identity thieves obtaining his/her PII. Under the circumstances, the overwhelming inference is that the identity theft was a direct and proximate result of the 2013 Breach.

73. Notwithstanding Officer Vigneault's efforts to respond to the situation (for example, dealing with the IRS), there is nothing he can do about the fact that his PII was

disclosed to one or more criminals whose identity remains unknown, and that his PII will remain at risk, in the public domain, permanently nothing she can do about the fact that his PII was disclosed to one or more criminals whose identity remains unknown, and that his PII will remain at risk, in the public domain, permanently.

74. Ammi Rice is another former student in the District. As such, she provided her PII to the District, which would have included, among other things, her date of birth, name, address, social security number, current and former addresses, telephone numbers, email addresses, marital status, motor vehicle records information, place of employment, and financial information. Ms. Rice is a victim of the 2013 Breach, and submitted a Notice of Claim to the District on April 28, 2014.

75. In her Notice of Claim, Ms. Rice explains that she is a victim of identity theft as a result of the District's conduct. Specifically, one or more thieves with access to her PII filed a fraudulent tax return in her name, which only came to her attention when she received a letter from the IRS confirming that it had received "her" tax return (a return she had not yet filed).

76. Ms. Rice is vigilant in protecting her PII, takes reasonable precautions to keep it out of the public domain, and is unaware of any other breach or theft that could have been the source of one or more identity thieves obtaining her PII. Under the circumstances, the overwhelming inference is that the identity theft was a direct and proximate result of the 2013 Breach.

77. Notwithstanding Ms. Rice's efforts to respond to the situation (for example, dealing with the IRS), there is nothing she can do about the fact that her PII was disclosed to one or more criminals whose identity remains unknown, and that her PII will remain at risk, in the public domain, permanently.

78. Marjorie Cordry is another former student in the District. As such, she provided her PII to the District, which would have included, among other things, her date of birth, name, address, social security number, current and former addresses, telephone numbers, email addresses, marital status, motor vehicle records information, place of

employment, and financial information. Ms. Cordry is a victim of the 2013 Breach, and submitted a Notice of Claim to the District on April 28, 2014.

79. In her Notice of Claim, Ms. Cordry explains that she is a victim of identity theft as a result of the District's conduct. Specifically, a thief with access to her PII applied for and was approved as a co-signer on Ms. Cordry's credit card and incurred fraudulent charges on her account. She only learned of the theft when she called her credit card company on an unrelated matter, and was informed that the thief was listed as a co-signer on her account.

80. Ms. Cordry is vigilant in protecting her PII, takes reasonable precautions to keep it out of the public domain, and is unaware of any other breach or theft that could have been the source of one or more identity thieves obtaining her PII. Under the circumstances, the overwhelming inference is that the identity theft was a direct and proximate result of the 2013 Breach.

81. Notwithstanding Ms. Cordry's efforts to respond to the situation (for example, filing a police report and putting fraud alerts on her credit), there is nothing she can do about the fact that her PII was disclosed to one or more criminals whose identity remains unknown, and that her PII will remain at risk, in the public domain, permanently.

CLASS ALLEGATONS

82. Plaintiffs bring this action under Ariz. R. Civ. P. 23 on behalf of themselves and all persons or entities whose PII existed on the District's electronic information systems at the time of the foregoing events that led to the District issuing notice to class members (the "Class").

83. Numerosity. Plaintiffs believe that the Class includes millions of individuals and thousands of entities. Because most of the Class attended, worked for, or provided services at the community colleges and skill Centers in Maricopa County, Plaintiffs believe that the Class members are predominantly Arizona citizens, a fact that has been confirmed by the District's counsel. The Class is so numerous that joinder of all members in a single action is impracticable.

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

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

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

c. Whether the District complied with its obligations under A.R.S. § 41-4172;

d. Whether the District complied with its obligations under A.R.S. § 44-7501(A);

e. Whether the District has violated 18 U.S.C. § 2722

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

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

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

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

j. What was the nature and extent of the 2011 Breach;

k. What was the nature and extent of the 2013 Breach;

l. Whether the District's actions permitted unauthorized access to the PII of Plaintiffs and the Class members;

m. Whether the District was negligent in its failure to protect adequately the PII of Plaintiffs and the Class members;

n. Whether the District's conduct was reckless;

o. Whether the District's conduct was done knowingly;

p. Whether the District's electronic information systems remain unsecured from the same vulnerabilities that resulted in the 2011 Breach and the 2103 Breach;

q. Whether Plaintiffs and the Class members are entitled to compensatory damages against the District;

r. Whether Plaintiffs and the Class members are entitled to statutory damages under 18 U.S.C. § 2722(b)(1) against the District;

s. Whether Plaintiffs and the Class members are entitled to an award of attorneys' fees and reasonable costs under 18 U.S.C. § 2722(b)(3) against the District;

t. Whether Plaintiffs and the Class members are entitled to punitive damages against the District; and

u. Whether Plaintiffs and the Class are entitled to affirmative injunctive relief against the District.

85. Typicality. Plaintiffs' claims are typical of those of the other Class members. Plaintiffs' claims and those of the Class members have a common source and rest on the same legal and remedial theories. Plaintiffs have suffered similar injuries and

harm to the other Class members. Plaintiffs have no interests that are adverse to the interests of the other Class members with respect to the claims and issues in this suit.

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

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

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

COUNT 1

(Negligence)

89. Plaintiffs incorporate the allegations in paragraphs 1 through 88 above.

90. The District owed Plaintiffs and all Class members a duty of reasonable care in the handling, maintenance, and security of their PII

91. Through its acts and omissions, including those described above, the District breached that duty of reasonable care to Plaintiffs and the Class members.

92. As a direct and proximate result of the District's breach, Plaintiffs and Class members have suffered harm.

COUNT II

(Negligence Per Se, A.R.S. § 41-4172)

93. Plaintiffs incorporate the allegations in paragraphs 1 through 92 above.

94. The District owed Plaintiffs and all Class members a duty of reasonable care in the handling, maintenance, and security of their PII and other sensitive information.

95. Under A.R.S. § 41-4172, the District is required to develop and to establish commercially reasonable procedures to ensure that entity identifying information and personal identifying information collected or obtained by the District is secure and cannot be accessed, viewed, or acquired unless authorized by law.

96. Through its acts and omissions, including those described above, the District violated its obligations under A.R.S. § 41-4172, and, as a result, its duty of reasonable care to Plaintiffs and the Class members.

97. As a direct and proximate result of the District's breach, Plaintiffs and Class members have suffered harm and continue to suffer harm.

98. Upon information and belief, the District's IT systems and databases still remain vulnerable and unsecured. As reported in December 2013, a District student engaged in his own independent security investigation and located vulnerabilities in both July and December of 2013 that allowed him to access confidential PII on the District's IT systems. When asked whether "is it safe to say that all of the issues that have led to this breach have been repaired," District representatives replied "I don't know whether all of them have."

99. The results of the District student's independent investigation are corroborated by the Minutes of the District's Governing Board dated November 12, 2013, which reflect that the security vulnerabilities in the District's systems "will take approximately 18-24 months to fix." The Minutes further noted, "How can we justify to tax payers that it will take 18-24 months to fix while leaving us vulnerable to hacking."

100. As a result, the personal and confidential PII of Plaintiffs and the Class members continues to be compromised and exposed to being accessed, viewed, or acquired by unauthorized persons, in violation of A.R.S. § 41-4172.

101. In the absence of injunctive relief, Plaintiffs and the Class members continue to be subjected to irreparable harm – the exposure of their PII and ongoing potential for identity, credit, and financial theft.

COUNT III

(Negligence Per Se, A.R.S. § 44-7501)

102. Plaintiffs incorporate the allegations in paragraphs 1 through 101 above.

103. The District owed Plaintiffs and all Class members a duty of reasonable care to notify them in a timely manner if their PII or other sensitive information was potentially exposed to unauthorized access.

104. Under A.R.S. § 44-7501(A), once the District became aware of the 2013 Breach, it was required to provide notice to Plaintiffs and the Class members in the "most expedient manner possible and without unreasonable delay."

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

106. As a direct and proximate result of the District's breach, Plaintiffs and Class members have suffered harm. The District's unreasonable delay in providing notice left Plaintiffs and the Class members further exposed to identity theft for a significant period of time. It also denied them the opportunity to take earlier affirmative steps to protect their identities, accounts, and credit from access and theft.

COUNT IV

(Breach of Fiduciary Duty)

107. Plaintiffs incorporate the allegations in paragraphs 1 through 106 above.

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

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

110. As a direct and proximate result of the District's breach, Plaintiffs and Class members have suffered harm.

111. Because the District's actions were willful and wanton and in reckless disregard of the rights of Plaintiffs and the Class members, Plaintiffs and the Class members are entitled to an award of punitive damages.

COUNT V

(Bailment)

112. Plaintiffs incorporate the allegations in paragraphs 1 through 111 above.

113. The PII of Plaintiffs and the Class members is property that belongs to them and to no one else.

114. Plaintiffs and the Class members delivered their PII to the District in trust that the District would secure their PII and protect it from unauthorized access and disclosure.

115. Plaintiffs and the Class members delivered their PII to the District to use solely for purposes of their own personal education, financial aid, employment, or business with the District and for no other purpose.

116. Plaintiffs and the Class members had a reasonable expectation that the PII that they entrusted to the District would remain private and not subject to disclosure to, or to access by, unauthorized persons. In particular, Plaintiffs and the Class members had a reasonable expectation that the District would take reasonable efforts to ensure that their

private PII could not be accessed, viewed, or acquired by anyone other than authorized persons within the District.

117. The District accepted and even required such PII on the understanding that it would undertake reasonable efforts to ensure that the PII was secure and could not be accessed, viewed, or acquired unless authorized by law.

118. The District further understood, when it accepted the PII of Plaintiffs and the Class members, that it would have to account for any misuse or its failure to ensure that the PII was secure and could not be accessed, viewed, or acquired unless authorized by law.

COUNT VI

(Breach of the Right of Privacy)

119. Plaintiffs incorporate the allegations in paragraphs 1 through 118 above.

120. Under Article 2, Section 8 of the Arizona Constitution, Plaintiffs and the Class members have a right to privacy that may not be disturbed without authority of law.

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

122. The PII of Plaintiffs and the Class members is personal information concerning their private life and is protected by Plaintiffs and the Class members from public disclosure.

123. Plaintiffs and the Class members had a reasonable expectation that the PII that they entrusted to the District would remain private and not subject to disclosure to, or to access by, unauthorized persons. In particular, Plaintiffs and the Class members had a

reasonable expectation that the District would take reasonable efforts to ensure that their private PII could not be accessed, viewed, or acquired by anyone other than authorized persons within the District.

124. The private PII of Plaintiffs and the Class members is not of legitimate concern to the public and its exposure to the public would be highly offensive to a reasonable person. Indeed, private PII, like the private PII of Plaintiffs and the Class, is guarded by most members of the public precisely because that information is not of legitimate concern to the public and its exposure could have adverse effects.

125. Through its acts and omissions, including those described above, the District violated the rights of privacy of Plaintiffs and the Class members. As a direct and proximate result, Plaintiffs and the Class members have suffered harm and will continue to suffer harm, including but not limited to the ongoing exposure of their PII by virtue of the District's failure to correct the problems that resulted in the 2013 Breach.

COUNT VII

(Violation of 18 U.S.C. § 2722)

126. Plaintiffs incorporate the allegations in paragraphs 1 through 125 above.

127. Under 18 U.S.C. § 2722, it is unlawful for any person knowingly to disclose personal information from a motor vehicle record for any use not permitted under 18 U.S.C. § 2721(b).

128. Among the Plaintiffs' and Class members' PII that exists and is maintained on the District's electronic information systems is information from their motor vehicle records, including their Arizona driver license numbers.

129. After the 2011 Breach, the District was fully aware that the PII of Plaintiffs and of the Class members was not adequately secure and not adequately protected from access, viewing, and removal from the District's electronic information systems by third parties.

130. Moreover, the District ignored repeated warnings by District employees over an extended period of time that the PII remained essentially unprotected and subject

to disclosure to unauthorized persons and hackers. Given the events of the 2011 Breach and the failure to cure the problems resulting in that breach, the District was fully aware of the near certainty of future infiltrations and intrusions by unauthorized persons and hackers to obtain the PII of Plaintiffs and the Class members. Nonetheless, the District failed to take appropriate actions to fix the security of the electronic information systems and potential access to the PII of Plaintiffs and the Class members, knowing that disclosure of that PII would be inevitable.

131. Through its acts and omissions, including those described above, the District has disclosed the PII of Plaintiffs and the Class members for a use not permitted under 18 U.S.C. § 2721(b), and has thus violated 18 U.S.C. § 2722. As a direct and proximate result of the District's actions, Plaintiffs and the Class members have suffered harm.

132. Under 18 U.S.C. § 2724(b)(1), Plaintiffs and the Class members are entitled to recover actual damages, but not less than liquidated damages in the amount of $2,500 each.

133. Under 18 U.S.C. § 2724(b)(3), Plaintiffs and the Class members are entitled to recover their reasonable attorneys' fees and other litigation costs reasonably incurred.

134. Because the District's actions were willful and wanton and in reckless disregard of the rights of Plaintiffs and the Class members, Plaintiffs and the Class members are entitled to an award of punitive damages.

PRAYER FOR RELIEF

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

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

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

C. For injunctive relief requiring that the District take the necessary steps to ensure that the PII of Plaintiffs and the Class members is secure and cannot be accessed, viewed, or acquired unless authorized by law;

D. For actual damages, but not less than liquidated damages in the amount of $2,500 for each Plaintiff and each member of the Class pursuant to 18 U.S.C. § 2724(b)(1);

E. For an award of reasonable attorneys' fees and other reasonably incurred litigation costs pursuant to 18 U.S.C. § 2724(b)(3);

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

G. For punitive damages in an amount to be determined by the jury; and

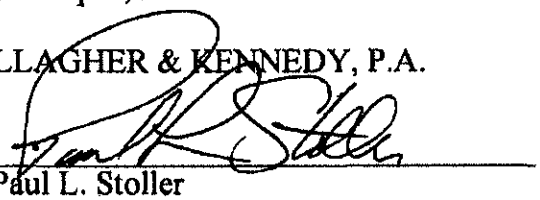
H. For such other and further relief as the Court deems appropriate.

DEMAND FOR JURY TRIAL

Plaintiffs demand trial by jury of all issues.

RESPECTFULLY submitted this 28th day of April, 2014.

GALLAGHER & KENNEDY, P.A.

By: 

Paul L. Stoller
Mark A. Fuller
Jeffrey T. Pyburn
Kiersten A. Murphy
Christopher W. Thompson
2575 East Camelback Road
Phoenix, Arizona 85016-9225

Attorneys for Plaintiffs

4179407v1/24656-0001