Gallagher&Kennedy

Mark A. Fuller
Shareholder
Direct: (602) 530-8185
Email: mark.fuller@gknet.com

December 27, 2013

VIA HAND DELIVERY

Mr. Dana G. Saar
Secretary
Maricopa County Community College District
Office of the Governing Board
2411 West 14th Street
Tempe, Arizona 85281-6942

Re: *Notice of Individual And Class Claims For Exposure of Private, Personal, Confidential Information*

Dear Mr. Saar:

This firm represents [redacted] ("Claimant"), individually and on behalf of a class of all persons similarly situated. Under A.R.S. §12-821.01, we are giving notice to the Maricopa County Community College District (the "District") of Claimant's and the class's claims against the District arising out of the lapse in security that allowed unauthorized access to private, confidential information of current and former students and applicants, parents of students and applicants, employees, vendors, and other individuals and businesses. [redacted] is a former student who recently received notice of the breach for the first time via what appears to be a form letter from the District. We understand that [redacted] is one of approximately 2.5 million people who has received, or will receive, this letter.

I. Factual Basis of Claim

The factual basis for the claims is as follows. The District operates ten colleges, two skill centers, and a number of other educational centers in Maricopa County. For years it has collected highly confidential, personal information from applicants and students, their parents, and others. The information is provided to the District to be held in the strictest confidence, and includes names, addresses, phone numbers, e-mail addresses, Social Security numbers, dates of birth, demographic information, and enrollment, academic and financial aid information.

Although the letter recently mailed to Claimant and other victims does not disclose this, we have learned that the Federal Bureau of Investigation notified the District in January 2011 that one or more of the District's databases were available for sale on the Internet. District employees were involved in the data breach. In addition, outside security consultants issued a report to the District

identifying significant security vulnerabilities. Notwithstanding all of this, the District did not take reasonable, adequate steps to protect against future, similar data breaches, and did not even notify the victims.

In April 2013, the FBI alerted the District – *again* – that confidential personal information collected by the District was available for purchase on the Internet. According to the District's outside counsel, the data breach involved *fourteen* databases. 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 while it conducted an internal investigation. Although the District has yet to reveal the details of the investigation, it has acknowledged that "an outside consultant" determined that the data breach "was due to substandard performance of [the District's] IT workers," and that the vulnerabilities that led to the breach "resulted from employee conduct that did not meet Maricopa's standards and expectations." In other words, the District has effectively conceded its own negligence.

It was only recently that the District finally began advising the victims of this latest breach, albeit in terms designed to minimize the threat and provide a false sense of comfort. In a form letter mailed to Claimant and approximately 2.5 million other 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 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 cannot actually determine that any victim's data was not, or will not be, misused. As if all of this were not misleading enough, the District 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, of course, 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 personal, confidential information exposed in this matter is tantamount to a gift-wrapped package for anyone seeking to steal someone's identity. There is no way to put that genie back in the bottle; the threat will follow each person for the rest or his or her life. Moreover, the threat is not merely an unauthorized credit card charge, but an identity theft with devastating impact on victims' lives.

In its letter, the District offers a kind of Band-Aid to the victims, stating that it will provide "identity safeguards and other services at no cost to you for one year through its ID TheftSmart

program." Even putting aside the fact that this "offer" requires affirmative action by the victims of the District's conduct and that it comes far too late, the offer is woefully insufficient to address the harm caused by the District. Fairly viewed, its only purpose is to give the victims a false sense of security by suggesting that the problem is short-lived and easily dealt with. Nothing could be further from the truth. In this internet age, the exposure of this kind of information requires affirmative, aggressive steps to protect every victim's identity plus long-term total identity monitoring (including an insurance component).

II. Legal Theories

Claimant is not in a position to articulate all of the bases for the District's liability at this stage. That said, the District has already publicly acknowledged the negligence of its employees, and it is plain that the District did, in fact, breach its duty of care to potential victims within the zone of foreseeable risk. *See, e.g., Rossell v. Volkswagen of Am.*, 147 Ariz. 160, 164, 709 P.2d 517, 524 (1985). The District has likewise acknowledged that its negligence was the cause of the data breach and thus the significant damage to Claimant and the other class members. The District is liable for the acts of its employees under the doctrine of *respondeat superior* and principles of agency. *See, e.g., Smith v. Amer. Express Travel Related Servs. Co.*, 179 Ariz. 131, 135, 876 P.2d 1166, 1170 (App. 1994); RESTATEMENT (SECOND) OF AGENCY § 228. Based on what we know at this stage, we believe the District will also be liable for negligent hiring, training, retention and/or supervision of the employees involved. *See, e.g., Kassman v. Busfield Enterprises, Inc.*, 131 Ariz. 163, 166, 639 P.2d 353, 356 (App. 1981); *Duncan v. State*, 157 Ariz. 56, 59, 754 P.2d 1160, 1163 (App. 1998); *Humana Hosp. v. Superior Court*, 154 Ariz. 396, 400, 742 P.2d 1382, 1386 (App. 1987); *In re Sproull*, 2002 Ariz. Lexis 45 (2002); *Natseway v. Tempe*, 184 Ariz. 374, 909 P.2d 441 (App. 1995); RESTATEMENT (SECOND) OF AGENCY § 213.

Negligence theories aside, Claimant and the other class members had a relationship of trust with the District, entrusting their private information to the District in strict confidence. The District invited such a fiduciary relationship, committing to protect the information and keep it safe. Through its conduct, the District violated its fiduciary duties.

Again, this is not meant to be an exhaustive list of the bases on which the District is liable to Claimant and the class. We are exploring and will continue to explore other bases for liability, and Claimant is not waiving his right to assert other theories, on his own behalf and on behalf of the class, if the case proceeds to litigation.

III. Sum Certain Demand and Its Basis

For purposes of A.R.S. §12-821.01, Claimant offers to settle his claim for the sum certain of $17,000, calculated as follows: (a) $1,000 to compensate for time and expense associated with initial steps to protect his identity; (b) $6,000 to compensate for the cost of procuring total identity monitoring for twenty years (at an average cost of $300 per year); and (c) $10,000 to compensate for the intangible loss of peace of mind caused by the knowledge that his personal, private, confidential information will remain at risk forever.

If the District wishes to settle this claim on these terms, please let me know within 60 days. Absent such a settlement, we intend to file suit not only on behalf of Claimant, but on behalf of the entire class of persons whose private, personal, confidential information was accessed without authorization.

Finally, we wish to remind you that the District has a duty under Arizona law to preserve any evidence related to this matter, regardless of whether the District believes the evidence is relevant. *See, e.g., Souza v. Fred Carries Contracts, Inc.*, 191 Ariz. 247, 250, 955 P.2d 3, 6 (App. 1997). This includes all information of any kind, in any form (physical or electronic), which is in the District's possession, custody or control and which refers or relates in any way to this matter, including but not limited to the data breach itself and the ensuing investigation(s).

Very truly yours,

GALLAGHER & KENNEDY, P.A.

By: Mark A. Fuller

MAF:dy