Gallagher&Kennedy

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

March 25, 2014

**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 lapses 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 the [redacted] and has been an adjunct faculty member in the District for a number of years. She received notice of the breach for the first time via what appears to be a form letter from the District. We understand that she is but one of approximately 2.5 million people who has received, or will receive, this letter, and has already suffered identity theft as a result of the theft of her private information.

## 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 as-yet-unidentified "enrollment, academic and financial aid information." We will refer to this as personal identifying information, or "PII."

Although the letter recently mailed to Claimant and other victims does not disclose this, the District learned in January 2011 from the FBI that one or more of its databases were available for sale on the Internet, and that its databases and webservers had been compromised allowing root and shell access to outside third-parties on multiple occasions dating back to April of 2007. As a result of these intrusions, databases containing confidential PII were for sale on the Internet. In the months that followed, District employees and outside consultants conducted a number of investigations that led to numerous reports outlining systemic and wide-ranging security concerns with District-wide information systems technology. The District, however, turned a blind eye to the threats, and even shut down investigations reflecting security breaches in other databases and servers by claiming that the evidence of such breaches were "false positives." Over and over 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 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 and faculty. The District did nothing.

In April 2013, the FBI alerted the District – *again* – that confidential personal information collected by the District was available for purchase on the Internet. This 2013 breach (the "2013 Breach") involved the same databases and webservers compromised in 2011. 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 apparently conducted an internal investigation of some kind. 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. Meanwhile, whatever "remediation" efforts the District undertook after being contacted by the FBI in April 2013 apparently destroyed the evidence as to what data was actually disclosed or otherwise made its way into the hands of others.

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 has no basis to say 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.

As we noted above, the District apparently destroyed critical evidence showing the extent to which PII was in fact misappropriated – a fact it neglected to tell victims in its form letters. [redacted] however, is among those who has *already* suffered the inevitable consequences of the breach. Although [redacted] 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 – information clearly obtained by the identity thief from the District's 2013 Breach. [redacted] was extremely fortunate in that she already had a PayPal account when the thief attempted to steal her identity. Because BillMeLater is affiliated with PayPal and PayPal had [redacted] email address on file with her existing account. The discrepancy between that email address and the one provided by the thief led BillMeLater to make contact with [redacted] directly, at which point she learned of the fraud. Nonetheless, [redacted] experience (and that of many other class members) confirms that the PII available on the internet was *in fact* misappropriated, has *in fact* has been misused, and will *in fact* be misused in the future. And notwithstanding [redacted] efforts to respond to the situation (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 confidential information will remain in the public domain *permanently*.

The District's letter to [redacted] and the other victims offers a kind of Band-Aid, stating that it will provide "identity safeguards and other services at no cost to you for one year through [Kroll's] ID TheftSmart program." Practically speaking, this "offer" is a sham. As a threshold matter, it comes far too late. The District did not even begin notifying victims until more than 7 months after the breach, and it is our understanding that even now, 11 months after the fact, notice letters are still being sent out. The offer requires affirmative action by the victims, the vast majority of whom the District knows are not likely to sign up. (In fact, as was widely reported in the press, many

GK

recipients viewed the letter as a scam.) One year is woefully insufficient; those who have the information know they can merely wait a year and start (or resume) using the data freely. And, Kroll's "protection" plan – presumably the result of a low bid – is anything but real protection. Ironically, [redacted] actually subscribed to the free offer, only to learn later that Kroll's "services" did not catch the BillMeLater incident. In fact, Kroll notified [redacted] that there had been no activity on her credit report well after she discovered the identity theft and fraud.

In short, the District's offer does not provide meaningful protection. To the contrary, it is the customary default marketing ploy used in data breach cases. The purpose is not to provide victims with what is actually necessary to try and mitigate the effects of the disaster, but to placate victims and imply 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 PII 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. As the District knows, it received public records requests from a variety of sources, including Claimant's counsel and the press, and has stonewalled at every turn. Claimant's counsel has filed suit to compel compliance with Arizona's Public Records law, but at this point, the District has remained steadfast in its refusal to abide its legal obligations under Arizona law, hiding many of the details about the data breach(es) from Claimants' counsel, the press, and the public at large.

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 duties as a fiduciary and a bailee.

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 (including potential claims for statutory damages), and Claimant is not waiving her right to assert other theories, on her 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 her claim for the sum certain of $24,000, calculated as follows: (a) $4,500 to compensate for time and expense associated with initial steps to protect her identity (an estimated 20 hours at an hourly rate of $225); (b) $6,000 to compensate for the cost of procuring total identity monitoring for twenty years (at an average cost of $300 per year); (c) $3,500 to compensate for the time Claimant has spent to date dealing with the effects of the breach; and (d) $10,000 to compensate for the intangible loss of peace of mind caused by the knowledge that her 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

GK