Before the
FEDERAL TRADE COMMISSION
Washington, DC 20580

In the Matter of)
)
Maricopa County Community College District)
)
_____)

Complaint, Request for Investigation, Injunction, and Other Relief Under the Safeguards Rule

Submitted by

"Dissent" (DataBreaches.net)
June 14, 2014

I. Overview

1. In January, 2011, **Maricopa County Community College District** ("**MCCCD**") – one of the largest higher education systems in the country - learned that access to one or more of its databases was up for sale on the Internet. Over the next two years, and despite repeated warnings from the state, its own personnel, and external consultants, MCCCD failed to fully remediate security vulnerabilities involved in that breach as well as other security vulnerabilities that had been identified both pre- and post-breach. As a direct consequence of their data security failures, employee, vendor, and student information was at risk of a similar attack or compromise. Predictably, then, MCCCD experienced a second breach in 2013. That breach involved the personal and financial information of almost 2.5 million people, making it the **largest breach ever reported by a U.S. institution of higher education**.[1] The breach caused substantial injury to employees, vendors, and students whose personal and financial information were exposed in the breach.

2. Because MCCCD had issued statements affirming their obligation to comply with the Safeguards Rule, and because student loan information was stored but inadequately secured, resulting in a reasonable likelihood of significant injury, the complainant believes MCCCD violated the **Safeguards Rule** (16 CFR 314) and its data security failures are actionable by the Commission. As outlined in this complaint, MCCCD's numerous unreasonable data security practices and failures are identical to those identified by the FTC in *Wyndham* and other cases as being unreasonable.

[1] Statistic based on almost 1,000 U.S. university and college breaches compiled at DataLossDB.org.

II. Parties

3. The complainant, **"Dissent"** (pseudonym), is a privacy advocate who publishes PogoWasRight.org, PHIprivacy.net and DataBreaches.net, three non-commercial blogs oriented to increasing consumer awareness of issues affecting their privacy. She is not employed in the field of security or privacy, but investigates data breaches and serves as a volunteer researcher and curator for DataLossDB, a project of the Open Security Foundation. This complaint is submitted in her personal capacity as a privacy advocate.

4. **Maricopa Community Colleges** consists of 10 colleges, 2 skill centers and numerous education centers. Each college is individually accredited, yet part of a larger system - the **Maricopa County Community College District ("MCCCD")**. According to their site, more than 265,000 students attend the Maricopa Community Colleges each year, taking credit and non-credit courses. In addition to its local offerings, MCCCD also offers numerous courses over the Internet and offers workforce opportunities or vocational certification. MCCCD describes itself as "one of the largest providers of higher education in the United States." As such, they have collected and stored a large amount of personal and sensitive information, including student loan information.

5. MCCCD offers a variety of financial supports for students, including, but not limited to, needs-based grants and scholarships, work-study programs, and loans that are repaid with interest. [2].[3]

6. In a number of their internal documents, MCCCD recognizes its obligation to comply with the Gramm-Leach-Bliley Act ("GLBA"), the Family Education Rights Privacy Act ("FERPA"), the Health Insurance Portability and Accountability Act ("HIPAA), the Red Flags Rule,[4] and the Safeguards Rule.[5] By their own statements, then, they were required to provide reasonable data security for the student financial loan information that they collected, processed, and/or stored.

7. MCCCD's administrative offices are at 2411 West 14th Street, Tempe, Arizona 85281.

III. Factual Background

A. The 2011 Data Security Breach[6]

8. In January, 2011, an employee discovered that a hacker, "srblche," had listed

---

[2] https:// maricopa.edu
[3] https://my.maricopa.edu
[4] http://www.maricopa.edu/publicstewardship/maricopasteward/fall2009/fall2009REV.pdf (p. 5)
[5] cf, http://www.maricopa.edu/its/Process%20%20DI%20Data%20Access%20Main%20Description.pdf, http://www.maricopa.edu/publicstewardship/pr/RIMHandbook2009.pdf http://www.maricopa.edu/publicstewardship/pr/RIMHandbook2012.pdf
[6] MCCCD had two breaches. The 2011 breach was not fully remediated, leading to or allowing the 2013 breach. Although the 2011 breach did not involve student financial loan information, the inadequate response to that breach set the stage for the 2013 breach that reportedly did involve student financial information.

www.maricopa.edu among government and educational sites to which he was selling access.[7] The FBI also reportedly notified an MCCCD Information Technology Services ("ITS") employee of the situation.[8]

9. Upon discovery of the situation, MCCCD ITS personnel reportedly immediately changed database login credentials and attempted to determine whether any personal information had been accessed and/or acquired. They also retained Stach & Liu (now Bishop Fox) to investigate what happened, and in cooperation with ITS personnel, determine the scope of the breach. Stach & Liu was also tasked to make recommendations and suggest mitigation strategies.[9]

10. Employees involved in investigating the incident have publicly stated that the web servers were compromised at the root level.[10, 11] They have also stated that the web server had likely been improperly accessed numerous (possibly hundreds) of times before they became aware of any breach in January, 2011.[12] Although the complainant was unable to confirm that allegation, state audits going back to 2007 had repeatedly noted problems with MCCCD's information security – problems that MCCCD repeatedly said it would address, but that were found unaddressed in subsequent audits.

11. There has been no public explanation by MCCCD as to why their systems failed to prevent or detect the 2011 breach. In non-public correspondence, however, employees have informed the complainant that prior to the 2011 breach, the network traffic monitoring system had been compromised, the network intrusion detection system was running - but poorly - and the firewall was configured improperly.

12. Throughout 2011 and into 2012, employees repeatedly urged MCCCD to replace the compromised server which left personal and sensitive information still at risk. When MCCCD failed to take their recommended steps, the employees filed an Oversight Report.

13. When MCCCD didn't respond to the Oversight Report, employees filed a Grievance Report[13, 14]

---

[7] http://www.databreaches.net/99-can-buy-you-a-unis-full-database-informations/ Inspection of the hacker's post suggests that what was being offered for sale was probably administrator or login credentials and not the actual databases with personal information. This hacker was known for his SQLi and brute force attacks to obtain login credentials.

[8] According to a statement by MCCCD's lawyers in November, 2013, the FBI reportedly notified MCCCD that one or more databases was up for sale on the Internet in January, 2011: http://doj.nh.gov/consumer/security-breaches/documents/maricopa-county-college-20131127.pdf.

[9] MCCCD has not made the Stach & Liu report available under public records requests, claiming the report is exempt from public records law due to personnel matters arising from the breaches.

[10] http://www.arizonadailyindependent.com/2014/02/25/mcccd-ignored-employees-warnings-security-breached/

[11] http://rickgalvanlaw.com/employment-law-blog/kroll-finds-employee-nothing-wrong-mcccd-blames-employee/

[12] Due to MCCCD's denial of public records requests, the complainant has not been able to determine the accuracy of this allegation that was contained in a potential class-action lawsuit.

[13] As reported by the media: http://www.abc15.com/news/let-joe-know/report-employees-called-mcccd-servers-high-risk-in-complaint-to-district.

(see Appendix B for redacted Grievance Report).

14. Based upon information and belief, the employees never received a substantive response to the grievance report.

15. Appendix A provides a partial chronology of developments, including numerous attempts by multiple employees throughout 2011 and 2012 to get MCCCD to address ongoing security vulnerabilities as well as state audits that also reported ongoing concerns.

B. **The 2013 Data Security Breach**

16. In what seems almost inevitable given that the server was reportedly still compromised by bad code, on April 29, 2013, the FBI contacted MCCCD again – this time to alert them that *14 databases with personal information* were up for sale on the Internet.

17. Despite the seriousness of the situation, MCCCD did not take the servers offline until May 15 - over two weeks later.[15]

18. In September, 2013, months before almost 2.5 million individuals would be notified of the breach, the *Scottsdale Chronicle* reported that my.maricopa.edu had been hacked, and that MCCCD brought the server back online after it was determined to be secure.[16] Others' statements, however, suggest that it still wasn't secure when it was brought back online after the 2013 breach,[17] just as the web servers were allegedly not adequately secured when they were brought back online following the January, 2011 incident.

19. Unfortunately, in their attempts to mitigate the severe 2013 security breach, MCCCD and/or its consultant reportedly destroyed records that could have confirmed whether data were exfiltrated or not, and if so, which data.[18] At the very least, it appears that 2.5 million

---

[14] One of the issues in the grievance alleges retaliation against ITS employees who disagreed with administration over the remediation of the 2011 breach. They allege internal conflict resulted in massive personnel firings and resignations that left MCCCD without an adequate pool of trained personnel in ITS at the time of the 2013 breach. The state audit in 2013, quoted in this complaint, also noted that the massive firings and resignations prior to the 2013 breach likely contributed to it.

[15] http://www.maricopa.edu/gvbd/archives/Agenda%20Jun%2013/062513/V.A.1%20Action%20Item_Stach%20&%20Liu_final060413.pdf. In this document, MCCCD says the Interim Chief Information Officer became aware of security vulnerabilities "the week of May 13," but MCCCD was notified of the breach on April 29. Why, then, did the Interim CIO not become aware of vulnerabilities until two weeks later – particularly when employees had been reporting them since 2011? Why the significant delay in taking the servers offline?

[16] http://www.scottsdalechronicle.org/features/server-issues-spread-throughout-maricopa-colleges-1.3062671?pagereq=1

[17] Months after the 2013 breach, MCCCD's servers were allegedly still vulnerable, as reported by a self-proclaimed "ethical hacker" to KPHO. http://www.kpho.com/story/24276899/ethical-hacker-maricopa-community-colleges-data-still-exposed

[18] Reported by MCCCD's external counsel to the New Hampshire Attorney General's Office: http://doj.nh.gov/consumer/security-breaches/documents/maricopa-county-college-

individuals' personal and financial information could have been acquired by criminals due to MCCCD's inadequate security.

20. In its notification to the New Hampshire Attorney General's Office of November 27, 2013, lawyers for MCCCD describe the types of information in the compromised databases:

> *MCCCD's systems contained sensitive information of MCCCD students, employees, and vendors. Employee information contained in the system included the following information: names, addresses, phone numbers, e-mail addresses, Social Security Numbers, dates of birth financial and bank account information, certain demographical information, information related to employment, education and training, and limited benefits information, including plan selection, vacation accrual, or dependent's information. The systems contained the following information pertaining to MCCCD's students: names, address, phone numbers, e-mail addresses, Social Security Numbers, dates of birth, certain demographical information, and enrollment, academic, and financial aid information. Vendor information included names, business names, addresses, Federal Employer Identification Number, and bank account information.*[19]

With 2.5 million notified, the MCCCD currently stands as the largest breach ever involving a university. Yet while Congress called the University of Maryland to testify about their breach[19, 20] - which affected far fewer people and did not involve financial information - no Congressional committee has investigated the MCCCD breach and no federal agency has stepped up to ensure that MCCCD is held accountable for its unreasonable security.

21. MCCCD's notification to those affected - which they did not provide until seven months after being notified of the breach by the FBI - did not disclose that there had been a previous breach in 2011 that had never been completely mitigated or that the FBI had found 14 databases up for sale on the Internet.[21] By withholding that information, MCCCD deprived those affected of information that might help them gauge their risk of ID theft and determine what steps they should take to protect themselves. Instead, the notification letter attempted to lay the blame for the breach on the substandard performance of ITS employees.[22]

22. In addition to destroying important information in attempting to mitigate the 2013 breach,

---

20131127.pdf. Their filing also contains copies of the notification letters sent to employees and students.

[19] http://www.databreaches.net/university-of-maryland-discloses-data-breach-involving-309079-records/

[20] http://www.wusa9.com/story/news/local/2014/03/26/university-of-maryland-congress-data-breach/6942023/

[22] The Kroll report cited by MCCCD's external counsel in their notification to the New Hampshire Attorney General's Office has not been made publicly available. It has been criticized by numerous current and former employees as an attempt to scapegoat or as a pre-determined "witch hunt." At the very least, it seems probable that Kroll did not interview all parties with important and firsthand knowledge: http://www.arizonadailyindependent.com/2014/02/25/mcccd-ignored-employees-warnings-security-breached/. The attorney for one of the employees who was blamed for the breach tells his client's side of the story and about Kroll's interview here: http://rickgalvanlaw.com/employment-law-blog/kroll-finds-employee-nothing-wrong-mcccd-blames-employee/

MCCCD may have also destroyed other records. Their Legal Department seemingly did not instruct ITS to preserve evidence until January, 2014, and that message wasn't relayed to personnel until weeks later.[23] It is not known to the complainant whether there was any incident response plan in place at the time of the 2013 breach and/or whether it was followed with respect to these records.

23. Although MCCCD claimed in their November, 2013 notification letter that they were not aware of any theft or misuse of the personal information, a number of people have since filed notices of claim against MCCCD, claiming that they became victims of ID theft or fraud as a result of MCCCD's breach.[24]

24. As a result of MCCCD's inadequate security policies, programs, and remediation of the 2011 breach, MCCCD has now spent almost $20M in lawyers' fees, consultants' fees, credit monitoring services, and security upgrades. They have recently imposed a tuition increase to raise revenues. The complainant believes that any tuition increase to raise funds that were spent due to their avoidable security failures constitutes significant and avoidable injury to current students.

IV. Prayer for Investigation and Relief

25. Based upon information and belief, because MCCCD and/or its Governing Board:

- did not sufficiently minimize data and retained unencrypted personal information on students, employees, and vendors for decades, including student financial loan information[25];
- allowed data to be vulnerable to common attacks such as Structured Query Language (SQL) injection;
- failed to have a properly configured firewall at the time of the 2011 incident;
- failed to have properly operating intrusion detection systems;
- failed to ensure that it had functioning intrusion prevention systems;
- failed to scan for vulnerabilities for almost a year (see Chronology, Appendix A);
- failed to remedy known security vulnerabilities, including hundreds of viruses detected by a vulnerabilities scan (see Chronology, Appendix A);
- brought a server back online in 2011 even though it still contained compromised code that it had not remediated;
- failed to implement the recommendations of its own personnel's strategic plan that had recommended common and industry-standard approaches to good data security;
- failed to implement the recommendations of its consultants who warned them of the risks associated with their security deficiencies;

---

[23] See internal MCCCD memo to staff included in the complainant's post at http://www.databreaches.net/arizona-law-firm-files-notice-of-claim-over-maricopa-county-community-college-district-breach-class-action-lawsuit-to-follow/

[24] Cf, this potential class action lawsuit: http://www.gknet.com/assets/4-28-14-Class-Action-Complaint.pdf. This is one of two potential class-action lawsuits that have been filed to date.

[25] Some commenters reported that they had not attended MCCCD since the 1970's: http://www.databreaches.net/maricopa-community-colleges-notifies-2-5m-after-data-security-breach/

- failed to implement data security recommendations of numerous state audits that they stated they would implement;
- failed to have an incident response plan in place;
- failed to have a Chief Information Security Officer;
- failed to schedule and conduct regular security audits;
- brought a still-compromised system back online in 2013 even though their consultants said it would take another year or more to really fix the problems[26];
- misinformed stakeholders that the systems were secure when they were not secure;
- failed to have an adequate staff of highly trained ITS personnel due to numerous firings and resignations that resulted from the 2011 incident and disputes over how to secure MCCCD's data assets;
- failed to timely notify those affected by the 2013 breach;
- failed to disclose that personal information was up for sale on the Internet;
- failed to respond to an employees' oversight report in 2011 that outlined data security concerns;
- failed to respond to an employees' grievance report in 2012 that included the ongoing data security concerns; and
- assured students that information submitted through their web server would be kept confidential and protected even when MCCCD knew that the server had already been compromised,

almost 2.5 million current and former students, vendors, and employees were exposed to risk of significant injury that they could not prevent and that was not otherwise offset by any benefit received, and some customers and consumers reported becoming victims of ID theft or fraudulent use of their information.

Because their security policies, programs, and practices were inadequate to protect student loan and financial information, the complainant believes MCCCD violated the Safeguards Rule and their conduct is actionable by the Commission.

Recent research by Risk Based Security and the Open Security Foundation reports that the education sector (primarily universities) is the second largest sector in terms of the number of entities where we have seen repeated data security breaches.[27] The MCCCD breach seems to epitomize this problem. Like the *Wyndham* case, inadequate security plus failure to properly remediate security vulnerabilities resulted in the likelihood of significant injury to consumers and customers.

---

[26] MCCCD brought servers back online in May 2013, telling the media that they were secure, when in fact, the board approved a contract with Eagle Creek in July 2013 to remediate web coding that it knew was not secure enough: http://www.maricopa.edu/gvbd/archives/Agenda%20Jul%2013/072313/V.B.1%20BOARD%20INFO%20ITEM%20Eagle%20Creek%20Web%20Services.pdf . That contract was expanded in November 2013: https://www.maricopa.edu/gvbd/archives/Agenda%20Nov%202013/112613/V.A.1%20Action%20Item_Eagle%20Creek_110713.pdf Eagle Creek noted that it would take another year or more to get everything working properly: http://maricopabreach.com/employment-law-blog/mcccd-may-still-risk-another-breach/

[27] https://www.riskbasedsecurity.com/reports/2014-1QDataBreachQuickView.pdf

26. Should the Commission determine that MCCCD has violated the Safeguards Rule, the Commission should require MCCCD to improve its data security practices and should provide such other relief as the Commission finds necessary and appropriate, including any civil monetary penalties for any officials who allowed unencrypted personal and student loan information to remain at risk of compromise for over two years because they did not comply with the requirements of the Safeguards Rule.[28]

27. The complainant reserves the right to supplement or amend this petition as other information relevant to this proceeding becomes available.

28. Should the FTC require any additional information from me, you may reach me via e-mail to admin@databreaches.net.

Respectfully submitted,

"Dissent"

[28] The complainant notes that the Governing Board had been made aware of concerns as early as 2012 and had been urged to arrange for an independent investigation of the ITS department, its dysfunction, and alleged retaliation by Vice Chancellor George Kahkejian, but had not done so. See the statements of Linda Brown, appended at pp. 10 -11 of the MCCCD Governing Board minutes of their meeting of January 28, 2014: https://www.maricopa.edu/gvbd/agenda/IV.A.1.a 01.28.14 Regular Board Meeting Minutes.pdf

APPENDIX A

Partial Chronology

January 2011: MCCCD learns that its web server has been compromised and access to at least one database is up for sale on the Internet in an underground market. ITS personnel change database login credentials and begins to investigate breach.

January 2011: MCCCD retains Stach & Liu to investigate breach and make recommendations for remediation. MCCCD would later claim that Stach & Liu's written report about the 2011 breach was never provided by ITS employees to MCCCD administrators "at the highest level."[29,30] At the time of the 2011 breach, however, MCCCD reportedly had no Chief Information Security Officer (CISO) or single person in charge of IT security,[31] even though an IT Services Department Assessment report conducted by LBL Technology Partners in January 2009 had recommended establishing that position.[32] A *Strategic and Operational Plan* for the district's ITS for 2009-2014 had also recommended creating a CISO position.[33] According to Miguel Corzo, who authored the latter plan, the plan was not adopted nor implemented by George Kahkedjian, Vice-Chancellor of ITS. Because there was no CISO and – according to several employees who spoke with the complainant - no incident response plan, it is not clear to the complainant whose responsibility it would have been to deliver a copy of the Stach & Liu report to MCCCD's governing board and Chancellor, but several ITS employees report that the Stach & Liu report *was* timely given to Vice-Chancellor of ITS George Kahkedjian in 2011.

January 25, 2011: A memo sent by George Kahkedjian, Vice-Chancellor of ITS, confirmed that there had been a breach:

> *By the end of last week we did find evidence of unauthorized access into our web hosting (Internet) presence. We have taken steps to mitigate risks as a precautionary measure. By Friday afternoon, we have found no strong evidence that personal/privacy information has been accessed or compromised in any of the databases. However, there is evidence that one file outside of our mission critical systems might have been exposed. Being exposed does not*

---

[29] MCCCD's claims that they never saw the report are somewhat astonishing, given Vice-Chancellor of ITS George Kahkedjian's March, 2011 memo to the Maricopa community about the breach, which suggested that the Vice-Chancellor was very much aware of the breach and what was being done in response to it.

[30] A timeline of events compiled by current and former employees involved in the IT department can be found on http://maricopabreach.com, a site created by the lawyer representing two employees against whom MCCCD took disciplinary action. A direct link to the timeline: http://rickgalvanlaw.com/employment-law-blog/mcccd-security-breach-timeline-events/ An article in the *Arizona Daily Independent* also offers a partial timeline: http://www.arizonadailyindependent.com/2014/03/03/mcccd-policies-ignored-glasper-staff/

[31] http://www.arizonadailyindependent.com/2014/02/25/mcccd-ignored-employees-warnings-security-breached/

[32] The LBL report, which is not available online, was sent to the complainant by a former employee. It also notes that at that time (January 2009), MCCCD did not have a security incident response plan. The same employee informed the complainant that at the time of the 2011 incident, there was still no incident response plan in place.

[33] http://www.docstoc.com/docs/39265783/Strategic-and-Operational-Plan-Information-Technology-Services-2009

necessarily mean that the data were breached. It only means that the file was in an area where it should not have been, and it must be carefully dealt with. The file has an extremely few number of records. We will follow the appropriate processes to address this matter as we move forward.

March 21, 2011: Memo by George Kahkedjian, Vice-Chancellor of ITS states that the exposed file contained names and Social Security numbers of approximately 250 MCCCD employees, who had been notified of the possible exposure.[34,35]

Throughout 2011, Kahkedjian was reportedly kept apprised of progress – or lack thereof – in remediating the 2011 breach. As one example, former employee Martin Gang subsequently wrote, in part:

> *As a direct result of the investigation and consultant's [Stach & Liu's] report, Rod Marten was tasked to replace the web server. He originally believed he could easily replace the system in two weeks. After his initial efforts he discovered the system was heavily interconnected. Rod then announced he believed that Maricopa ITS should instead purchase the web environment using a SaaS provider. After presenting his proposal to George Kahkedjian in late April 2011, George accepted the proposal and Rod and I were both tasked with working directly with Marketing and Public Relations to identify system requirements. As the process continued with no results I shared my concerns, first with Rod and then with George, that the system must be replaced as it had been so severely compromised that there was no genuine assurance that it was clean. When I left in November 2011, my understanding that Rod would have a new secure web environment by January 2012.*[36]

By April 2013, the system still had not been replaced and the personal information of millions of students, employees, and vendors remained on a system that ITS personnel believed posed a serious risk to security.[37]

November 2011: The 2011 breach does not appear to have been disclosed to state auditors, as it is not mentioned in their report. The audit discussed security concerns that the District was advised to address, noting that "*during fiscal year 2011, the District had not adequately implemented policies and procedures for granting access and making changes to its computer systems*" that included the system that housed the student information system. The effect of this, the state wrote, was that:

> *Inadequate controls could lead to an increased risk of theft, manipulation, misuse of*

---

[34] http://maricopabreach.com/wp-content/uploads/2014/04/GeorgetoMaricopa2011-1.pdf.
[35] The *Arizona Republic* subsequently reported that up to 400 employees were affected: http://www.azcentral.com/story/news/local/phoenix/2014/02/25/failure-to-address-2011-hacking-tied-to-13-breach/5800071/
[36] Gang's full statement was provided to the complainant by a former employee. Other portions of his statement are included in this media report: http://www.arizonadailyindependent.com/2014/02/25/mcccd-ignored-employees-warnings-security-breached/
[37] The personal information was not confined to current employees, vendors, and students. As reported by some recipients of the 2013 breach notification, personal information of some individuals who had not attended MCCCD for over two decades was on the compromised server.

sensitive or confidential information by unauthorized users, or unauthorized changes or changes that were not made accurately. This finding is a material weakness in internal control over financial reporting.[38]

The audit also noted that (emphasis added by complainant):

During the fiscal year, the District updated its policies over access and change management controls to address deficiencies noted in the prior year's audit. However, not all of these policies were implemented during the fiscal year, and the policies did not address all deficiencies noted in the prior years.

The District's response to the state audit was that it agreed with the recommendations and would address them. By April 2013, they still had not been fully addressed.[39]

November 2011 (estimated): Employees deliver Stach & Liu report to Vice-Chancellor of ITS.

November 2011: According to employees who spoke with the complainant, in November, employees were (finally) able again to run some vulnerability scans. But according to allegations in a class-action lawsuit filed after the 2013 breach, a supervisor dismissed the findings and report of the employee who ran Nessus scans that uncovered over 200 vulnerabilities.[40] Because the supervisor allegedly dismissed the scan results as not real vulnerabilities, they were likely never addressed.[41]

November 2011: Because the compromised server had not been replaced by 10 months after MCCCD learned of the 2011 breach, some employees submitted an oversight report to MCCCD.[42, 43]

---

[38] http://www.azauditor.gov/Reports/Community_Colleges/Maricopa_County_CC/Financial_Audits/IC_Control_and_Compliance_2011/Maricopa_CCCD_06_30_11_Rpt_on_IC.pdf

[39] This appeared out to be a recurring pattern. Every state audit pointed out problems that had not been addressed from previous year(s). Each year, MCCCD agreed and said it would implement the recommendations, but the next year's audit still found unaddressed problems.

[40] See http://www.gknet.com/assets/4-28-14-Class-Action-Complaint.pdf Paras 32-34.

[41] The supervisor, who also allegedly aborted some other aspects of the investigation following the 2011 incident, recently resigned. He was not one of the employees against whom the district took disciplinary action following the 2013 breach.

[42] The oversight report has not been made publicly available but in a timeline of the breaches constructed by employees, they state that the report included cautions that the webservers compromised in 2011 had not yet been fixed and that OVIS Tools to monitor the network and servers in Maricopa were still not operational. The report stated, in part: *"After 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."* The oversight report also discussed MCCCD's failure to timely complete replacing the LEGATO backup system, despite the risk to MCCCD of having a backup system that could (and did) fail and that had numerous incompatibilities.

[43] In March, 2014, MCCCD told a reporter from the *Arizona Republic* that they had no record of ever receiving the oversight report, but the individual to whom it was allegedly addressed and delivered would not respond to the newspaper's questions: http://www.azcentral.com/story/news/local/phoenix/2014/02/25/failure-to-address-2011-hacking-tied-to-13-breach/5800071/

The employees inform the complainant that they never received a response to that report.

March 6, 2012: Vice-Chancellor Kahkedjian provided the Governing Board with an "Update on Information Technology Strategic Plan & Governance."[44] The board's minutes of his presentation state:

> *We are very consistent with the industry regarding technology controls, managerial and operational controls. It is a constant balancing act protecting data. We cannot control adding cost to security. Operating and data security are problems because systems are not operating at full capacity. Students being impacted. Costs and corporate level controls need to be balanced. Security has been worked with very carefully. Managerial controls work with operations. Very good about where we are but we have a lot of work to do.*

Any claims that MCCCD was "very consistent with the industry" or "very good about where we are" strike this complainant as deceptive, at best, in light of all the unremediated vulnerabilities and outdated, misconfigured, or nonfunctioning controls.

October 2012: Employees file Grievance Report concerning ongoing security concerns and other matters, including lack of adequate IT personnel to address security concerns. (Appendix B has a redacted copy of the grievance report).

November 2012: State auditor report on *Internal Control and Compliance for the District, for the Year Ended June 30, 2012*[45] found 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.*" Again, the District indicated that it agreed with the auditor's findings and would take action. Yet again, it didn't.

April 29, 2013: District contacted by FBI who report that at least 14 databases with personal and sensitive information are up for sale on Internet.

May 15, 2013: MCCCD takes compromised servers offline.

November 2013: A state audit[46] for the fiscal year ending June 30, 2013 notes ongoing and serious security issues:

> *The District should strengthen its information system access and change controls*
>
> *Criteria: The District should have effective system access and change controls to help prevent and detect unauthorized use, damage, loss, or modification of systems and data, and misuse of*

---

44 https://www.maricopa.edu/gvbd/minutes/2012mins/3.6.12%20Board%20Work%20Session%20&%20Exec%20Session.pdf

45 http://www.azauditor.gov/Reports/Community_Colleges/Maricopa_County_CC/Financial_Audits/IC_Control_and_Compliance_2012/Maricopa_CCCD_06_30_12_Rpt_on_IC.pdf

46 http://www.azauditor.gov/Reports/Community_Colleges/Maricopa_County_CC/Financial_Audits/IC_Control_and_Compliance_2013/Maricopa_CCCD_06_30_13_ROIC.pdf

confidential or sensitive information.

Condition and context: The District has three primary information systems it uses to initiate, record, process, and report financial, human resources and payroll, and student information. However, the District did not adequately control access and changes to these systems during the year. Specifically, the District did not establish accountability and monitor system access and activities of users with elevated and unlimited system access. In addition, the District allowed database administrators and other users to have the ability to make data and system changes without being detected and without having accountability for the changes. Further, the District did not always follow its existing procedures for approving system access.

Effect: There is an increased risk that unauthorized access and changes to the District's systems, including financial information and data that is confidential or sensitive in nature, may not be prevented or detected. Such an occurrence can be very costly. In April 2013, the District's network security was breached by hackers resulting in estimated costs of $16.8 million to remedy vulnerabilities within its information systems and provide credit monitoring to an estimated 2.6 million individuals whose personal information may have been compromised.

Cause: The District did not have adequate policies and procedures to limit and monitor users with elevated and unlimited system access, including the ability to make data and system changes. In addition, the District did not follow its procedures to ensure all user access requests are properly approved by the user's supervisor. Further, the District's progress for improving its systems' access and change controls had been impeded by turnover in its Information Technology leadership and the need for consistent priorities on taking corrective action.

[…]

And once again, the auditors pointed out "*This finding is similar to a prior-year finding.* "[47]

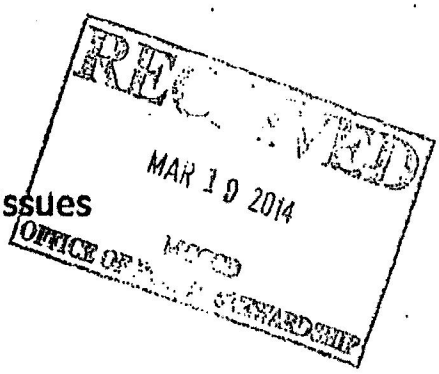
November 2013: MCCCD begins notifying almost 2.5 million affected by breach.

April 9, 2014: Employees escalate the Grievance Report to the Governing Board, who had 30 days to reply. Employees inform the complainant that the Governing Board did not respond.[48]

[47] http://www.azauditor.gov/Reports/Community_Colleges/Maricopa_County_CC/Financial_Audits/IC_Control_and_Compliance_2013/Maricopa_CCCD_06_30_13_ROIC.pdf

[48] A copy of the escalation e-mail can be found in Appendix C of this complaint.

APPENDIX B



Events Documentation

Violations of Policy and Non-Policy Issues

Stewardship Issues

A significant number of Board Approved projects are/have been behind schedule and over budget

Several Board approved projects like HR, SIS, CFS, Grants and others have routinely been behind schedule and over budget. The most notable project is the CFS upgrade and Grants. This project is now several years behind schedule and over budget.

The CFS project presents many stewardship challenges that fall under the responsibility of the [redacted] and the [redacted] (see attached)

- The project is significantly over budget and incomplete as of 9/24/12 yet the Governing Board has not been notified and/or a new project budget request sent to the Board.
- Operational dollars in the amount of $245K to Teksystems, Inc. should have been considered capital and not operational spending.
- As of September 2012, the project is over $1 million dollars over budget
- As of September 2012, the project expense is at $2million dollars and the project is at 50-75% completion.
- Consultants for this project have come and gone and the project has been extended for years beyond the initial Board approval date.
- Spending against the project budget continues w/o Board approval for increase project dollars.
- The original project estimate from the August 25, 2009 was $530,000. A new project was later approved by the Board on December 14, 2010 for $1,562,400. This represents a miscalculation on project budget of nearly $1 million dollars.
- The original Board proposal of August 25, 2009 presented a completion date of March 2011. The Board proposal of December 14, 2010 later moved that implementation date to Q2 2012. This represents over a year error in estimation of project completion.
- To this date, the project is yet to be completed and over budget. Current estimates point to Q4 2012 or Q1 2013 for implementation.
- No changes were made to the leadership of this project during this time and there was no accountability. In contrast, a [redacted] without any prior knowledge, experience or even a college degree was appointed to lead the project.
- The Board proposals for this project are misleading in nature. There were two proposals (see attached) one made in August 25, 2009 and another one in December 14, 2010. Both proposals are labeled CFS Release 12 Upgrade and CFS R12 Upgrade. In reality, the Board approved a 2009 CFS R12 Upgrade proposal for $530K. The project leadership failed to listen to the staff regarding estimates and they soon realized their mistake. The project leadership turned around

and created yet another proposal for $1.5 million. The Board was led to believe that this was a separate project based on the wording of the proposal. The Project Leadership team ended up spending the funds in the first and second proposals when in reality the second proposal should have been a request to increase budget/timeline for the first proposal in 2009. That was purposely left out of the wording. In addition, the project leadership had been so bad in estimating time and costs that they went from reporting months and years in a timeline to reporting quarters.

- It is clear that the second proposal contains the budget for the entire upgrade and funds from the first proposal should not have been used. The bottom of the third proposal clearly states "This schedule assumes Q1 2011 start..." This leads the Board to believe that they were funding a project that was to begin in 2011 not 2009.
- Funding for this project that should be coming from capital dollars are now coming from operational dollars that have not been approved by the Board. This is likely coming from salary savings in ITS.
- There are significant issues with the funding, management and planning for this project. A forensic investigation should be conducted into the finances that support this project and how it is being funded.

Another example of poor management and planning is the Grants Project (see attached)

- This Board approved project failed completely. The Board approved $364K for the completion of this project. A total of $394,830 was spent and there was nothing to show for.
- The Leadership of this project remained intact and there was no accountability for the failure.
- The project go-live date as proposed to the Governing Board on September, 2010 was December 2010. The project is now closed and nothing came out of it. The project failed and all funds were spent.

Consultants without direction [redacted]

In a meeting August 2012 between a consultant [redacted] and [redacted] asked the consultant who he was taking directions from. His response was, "No one at the moment. I am kind of self-directed." This is a consultant who is being paid with taxpayer dollars and is receiving no direction by his own acknowledgement. In recent communications with ITS, this consultant was assigned to work on a project regarding operational plans for all teams to later being removed from the project. The consultants spent many hours of his time and employees' time collecting information.

No management plan for consultants

As of September 2012, there are no management plans for consultant in place. It is unclear how consultants are being managed and what their charge/direction is.

Maricopa employees trained and then rehired as consultants

A current practice in the organization, which is rather unethical, is to hire individuals, send them to extensive training and wait for these individuals to leave the organization. Once they leave, they return back to Maricopa on a consulting basis at a higher pay rate. What is taking place here is that we are using taxpayer dollars to educate and train consultants that we will later rehire.

Ongoing retaliation and humiliation practices of senior ITS leaders present legal risks of MCCCD

Employees who recently filed discrimination complaints as a result of the practices followed during the ITS reorganization are being singled out and retaliated against. Low key actions such as alienation and isolation of these employees are taking place. Employees involved in EEOC complaints are not being invited to meetings and excluded from decision making. Employees involved in EEOC complaints are being moved out of their offices to make space for temporary consultants. Some of these employees now in leadership positions are being asked to move to cubicles as a form of silent retaliation. EEOC retaliation complaints are likely to be filed both internally and externally. This is a sign of the hostility and poor management environment employees are being subject to. Decisions out of the office of [redacted] to move employees are not being discussed with the top leadership [redacted] as acknowledged and witnessed by employees in a meeting.

Ignoring information from the Department leadership

SIS Upgrade failure

In an email sent to [redacted] prior to a major SIS rollout this spring, [redacted] clearly indicated to [redacted] that his DBA team was not in favor of a go-live date for SIS in the middle of the semester. His professional feedback was ignored and that of his team. The system went live and it was down for several days impacting faculty, staff and students across the District. In a letter obtained via records request and available for review, [redacted] blamed the DBA team for the failure of SIS in front of [redacted]. Here is the email. This email is supported by other communications to/from [redacted] They all indicate a reluctance to listen to the staff.

[redacted] sending this via text only. I talked to [redacted] about this communication with you so he is not surprise.

We have a very cordial disagreement in our recommendation for SIS. [redacted] and [redacted] are pushing a go-live, my staff is not. I am listening to the DBAs that have ran this system for many years without a glitch. They have invested a lot of time and energy into the Linux effort (more so than anyone) and see a lot of risk in going live.

My recommendation to you as my boss is that we delay until May. In addition to all the reasons I shared with you last week via my document, it appears that critical SIS members of the functional team are leaving for HEUG on Monday, our go live date. The most important factor driving my recommendation is lack of Linux resources at this time to guarantee uptime. Last but not least, the monitoring tools that we have used for years to help us troubleshoot production and monitor

performance are not operational.

The question is what is the sense of urgency? Is it real or self-imposed? Is middle of the semester a good time to do this with other issues brewing?

I believe that there are motives for this decision that may not include doing what is in the best interest of Maricopa. No one would acknowledge this but I have been around long enough to see it. We made that mistake before.

This is simply a difference of opinion in our degree of readiness and it has little to do with remaining technical issues, even though there are some.

I will support your decision and do everything we can to assist. My staff is moving forward helping the team as if we are going live.

I shared this perspective with [redacted] and while he agrees, he is choosing a different path. [redacted] believes we are ready. Again, this is just a cordial disagreement. I am not upset but I feel I have to share my perspective.

Thank you for listening.

Security Oversight Reports

A security oversight report was delivered to [redacted] by his [redacted] in the Spring of 2012. This report pointed out several risks and deficiencies in the organization. Most of the recommendations were ignored by [redacted]. The list of recommendations included:

- Resolution of web server compromises. Months passed and none of the agreed upon steps were resolved. This represented a high risk to the organization that could expose personal information.
- [redacted] over 3 years and approximately $1+ million dollars has been wasted on projects yet to be completed. The system has failed several times and there a numerous incompatibilities. The person responsible for this project has now been appointed [redacted] in the new ITS Reorganization. The risk to the organization was deemed to be high.
- Other projects like a monitoring system, stolen laptops etc... were brought up to [redacted] attention and little of nothing was done to address the risk to the organization.

Alienation and Isolation and favoritism

At the ELT meeting on 9/4/12 [redacted] indicated that she was working with [redacted] and [redacted] on staffing needs for the department. She indicated that the two main areas of concern were DBAs and Programming support for SIS. When questions were raised as to who they had talked to, [redacted] indicated that he had talked to DBA staff. Even though [redacted] has been in the office, he has never been approached regarding the staffing needs of his department. Multiple requests have

been made to fill open positions in the DBA team and no response has been received. There is a push by [redacted] to retain and extend the services of the Burgundy Group, a consulting firm providing DBA support. The lack of movement in the rehiring of new DBAs, the emphasis on expanding the services of the Burgundy Group and the persistent nature of this engagement is causing undue stress in the DBA team.

Leadership meetings are taking place and no transition period is being allowed even at a time of crisis. This is another indication of the retaliation and discrimination taking place in this hostile environment.

Unfair job assignments and favoritism

[redacted] was appointed to [redacted] to justify his upgrade yet he has no education or experience leading an ERP system. His current education is a GED diploma and he has never led a system like CFS. Others in the department had that experience and were not given the opportunity. The CFS project is behind schedule and over budget.

Individuals were assigned to positions in the new organizational structure that had no job descriptions associated with it. Titles did not even exist in HR at the time the reorganization took place 7/23/12. Individuals were appointed to these positions without an internal competitive process. For example, a meeting with HR on 9/11/12 was meant to 'define' the responsibilities of [redacted] new job, a job and grade I was assigned back in July 2012. See internal HR Letter regarding "Urgent – Create Job Descriptions," available upon request.

New organizational structure did not consider performance, past contributions, experience, education or any other key factors usually taken into consideration in a reorganization. Instead, this reorganization was purely based on favoritism and friendships. A perfect example is the [redacted], an individual close to [redacted] who recently received a promotion to a Grade 19 in the organization. This individual only holds a GED certificate and has no other education. There are others in the department with Master Degrees, MBAs and other advance degrees capable of doing the job yet they are being demoted or denied opportunities.

As indicated by [redacted] several emails (May 11, 2012), the reorganization is structural in nature yet some individuals are being upgraded while others are being downgraded. In official record requests obtained by MAT and PSA Presidents, there is no justification for any of the upgrades or downgrades. This speaks to downgrades/upgrades being done on the bases of favoritism and unfair job assignments.

The new organizational structure could have been possible without the need to downgrade anyone in the organization. Downgrades were punitive in nature and targeted at employees at or near retirement. As indicated by email from the [redacted] office, downgrades and upgrades were not done based on performance, qualifications or education. It is unclear what these downgrades were based on other than age discrimination, profiling and targeted punishment of certain employees.

Downgrade/Upgrades not justified

Records request found no justification for promotions, demotions that took place in the recent ITS reorganization. New positions that initially did not even have a job description were created to justify downgrades in the organization. The ITS reorganization apparently took place in July 23, 2012. To this date, September 24, 2012, several individuals in the organization still have not been told what their new role is. [redacted] per his request and own initiative, has scheduled a meeting with [redacted] for September 25, 2012 to discuss his new role and responsibilities

Upgrades and appointments were done w/o a competitive process in place. Individuals responsible for major system failure such as Canvas and SIS hardware upgrade received a promotion or were simply left intact.

Recently (8/26/12), [redacted] an individual who recently was downgraded, was asked to manage the CFS project and the consultants associated with it, while [redacted] was on vacation.

A[redacted] overseeing two District Office Innovation of the Year awards, was downgraded as part of this reorganization, claiming a need to improve customer service. These two innovation of the Year projects were recently recognized for saving MCCCD millions of dollars, improving customer service, and supporting the One-Maricopa Vision of the Chancellor.

The highest ranked Hispanic in the ITS organization was recently downgraded without cause. Several employees in non-protected classes were promoted without a competitive process in place. Others demoted like [redacted] were offered a position of leadership in the organization, reporting directly to the [redacted] nd with one direct report. While this may appear as a demotion in grade, it is a promotion in terms of scope. The only reason provided was that the move was necessary to improve customer service.

Preferential Treatment/Favoritism

In the recent ITS reorganization, [redacted] re still part of leadership team, yet [redacted] were removed from the leadership roles as a form of punishment. [redacted] both hold advanced Master Degrees and extensive experience running Enterprise Systems. [redacted] has received numerous recognitions as CIO of the Year in InfoWorld. Other individuals in the leadership team who still report to [redacted] o not have the experience, training and education necessary to perform the job. One of these employees, [redacted] holds a GED, another only has an Associate Degree. This leads us to believe that preferential treatment and favoritism is playing a role in this reorganization.

[redacted] was offered an OYO grade 19 to run CFS, yet he had not prior knowledge or experience of the system. In contrast, there are others in the department at lower grade levels with advanced degrees.

[redacted] was offered a grade 20 for a position he has no experience with and had not done before. In his new role, [redacted] still reports to [redacted] sits on the leadership team and only has one employee

reporting to him. In contrast [redacted] and [redacted] were both downgraded to a Grade 19, have three or more employees reporting to them and are no longer part of the Leadership team. The failure of projects like SIS, HR, CFS, Blackboard were the responsibility of [redacted] the Executive over those projects, yet it appears that favoritism is the reason why punishment is being imparted the way it is.

[redacted] a close friend of [redacted] was offered a closed-wall office when others in the department with higher grades reside in cubicles.

Discouraging people from applying

In a meeting with [redacted] direct reports, [redacted] and [redacted] indicated to the individuals present that they should not bother applying for the CIO/CTO. These positions were not meant for anyone in the room. As a result, only external candidates are being considered for the job. This denied opportunities to minorities and other protected classes.

Denied opportunities by not posting CTO positions and hiring for this position out of the CIO pool. These positions are responsible for two different areas in the organization. Experience in these areas appear not to be necessary to hire for these jobs.

On information revealed by records requests, it is clearly stated that [redacted] reorganized the department and placed people in positions that required certain specialized expertise. However, he demoted some individuals whose expertise was highly sought and who had years of experience, knowledge and education in Maricopa. There was no justification for upgrade, downgrades etc.

Processes not followed

No job descriptions. As of this date 9/24/12, several employees who have been reclassified do not know what their new job function is. The reorganization took place 7/23/12.

No performance expectations. Employees have been downgraded in the organization without due process. Performance expectations were not set with any of these employees.

No negative evaluations. None of the employees downgraded had any form of negative evaluations in their years of service at Maricopa.

No corrective action. No corrective action was initiated for any of the employees downgraded.

No proper notification. Notifications and policy violations took place as part of the reorganization. Employees were not notified in time. Once HR recognized their mistakes letter were delivered to employee homes. In some cases, unsealed letters were delivered to children at the house of employees impacted. In other cases, letters were left under a mat at the employee homes.

Unethical behavior

Upon realizing their mistake, the HR organization made changes to the system, erase information to cover their tracks and over paid individuals in the system.

Ignoring process for selection of SIS Architecture (highest scoring proposal). An internal process was developed (documentation available) to select the best option for an SIS architecture upgrade. A scoring matrix was put in place and meetings were held with vendors and internal staff. A decision was made by [redacted] to bypass all scoring and work done on finding the best solution for Maricopa. The highest ranked recommendation was ignored. As a result, SIS was up and down for a week and has experienced multiple failures since the upgrade in the Spring of 2012. Downtime for SIS means that faculty, staff and students are not being served.

[redacted] lied about SIS failure. In a letter to [redacted] obtained via records request, [redacted] blamed a Spring 2012 failure of SIS on the DBA team. [redacted] had been told several times by both [redacted] and members of the DBA team in group meeting that going live with an upgrade mid-year was not a good idea. The system failed at go-live and [redacted] blamed the DBA team. This is unethical behavior.

Discrimination

A Hispanic in the ITS organization requested a replacement computer multiple times (first request 3/25/2012) and [redacted] continued to ignore these requests. Others in the department have received new computers since. This behavior by the same employee led Maricopa in the past to have to settle another EEOC complaint.

The ITS reorganization has clearly impacted minority employees like [redacted] and [redacted] New positions were created and people assigned to roles without a competitive process in place. As members of a protected class, these individuals were denied opportunities for advancement.

There are significant issues with age and gender discrimination. A complaint regarding age discrimination was filed. Additional EEOC complaints regarding gender and race are likely to follow.

Intimidation

Threats made to [redacted] on July 3, 2012 by [redacted] where he said in front of [redacted] 'I am downgrading you because I can'

Threats made to all ITS in employee meeting by [redacted] In that meeting, he commented 'If you have to get a lawyer do so, you won't win'

Threats made to [redacted] by [redacted] when approached about the reorganization. "If you don't like it, leave."

In a public all ITS meeting, [redacted] told all of ITS that he would fire 40% of the department if it was up to him.

Threats made by [redacted] to direct reports indicating that the entire organization including EEOC, Legal, [redacted] and HR were aware and in support. Meetings with EEOC and Legal later confirmed that this was not the case.

[redacted] and [redacted] at a direct reports meeting with [redacted] and others as witness, clearly indicated to the staff that the new CIO and CTO positions were not meant for any of the direct reports [redacted] clearly discouraged anyone from applying to positions they were qualified for thus denying opportunities.

Most recently, two high-level positions were advertised (CIO/CTO). Two candidates were offered the job and both declined. This is a direct result of the hostility in this environment. No one wants to work at Maricopa IT. The consequences are rather severe in attracting qualified personnel.

Over 24 vacant positions exist in the Department since [redacted] rrived. These are people who either retired or resigned as a result of [redacted] agement style and reorganization. In addition, there are over 15 individuals on FMLA. This is yet another sign of the stressful and hostile environment that we are working under. Employees are resorting to taking sick time, leave of absences, medical leaves and other forms of time off to protect their health and recover from the stress this hostile environment has brought upon them. This translates to significant medical expenses for MCCCD, loss in productivity and low employee morale.

In a meeting between [redacted] and [redacted] prior to the ITS Reorganization becoming effective, [redacted] met with [redacted] seeking and explanation for his downgrade. [redacted] indicated that his demotion was not due to performance, that his skills were needed in a new job. He then proceeded to tell [redacted] that he should be happy that he had a box in the organization and that he did not have to spend the time to go through a hiring process with the risks that he may not be the selected applicant for the position.

Retaliation

[redacted] retaliated against [redacted] ugust 6, 2012 by destroying personal property in her work area. He proceeded to indicate that he was tired of her and her group. She felt threaten and intimidated. She requested to be moved and was disrespectfully treated. She was asked to go to another building when in reality there were plenty of open spaces in the department. To this date, Setpt24th, 2012 no action has been taken by the organization and [redacted] still remains in close proximity to the person that destroyed her personal property.

[redacted] was asked to remove a leadership flyer from his office wall by [redacted] when someone from the office complaint. There are many other cubicles and offices in the department with similar inspirational messages and no one else was asked to remove anything. This was a targeted retaliation attempt and should be investigated.

On Sept 21, 2012, after filing a discrimination complaint with the EEOC office, an employee involved in the EEOC complaint was asked to move from an office he has held for several years to a cubicle. Others

APPENDIX C

Note: Personal e-mail addresses redacted by the complainant.

From: Miguel Corzo <REDACTED>
Date: Wed, Apr 9, 2014 at 7:47 PM
Subject: Escalation of ITS Grievance to Governing Board Members
To: doyle.burke@domail.maricopa.edu,
alfredo.gutierrez@domail.maricopa.edu,
randolph.lumm@domail.maricopa.edu,debra.pearson@domail.maricopa.edu,
dana.saar@domail.maricopa.edu
Cc: ER M <REDACTED>, Gary Nusbaum <REDACTED>, Chris
Millanez <REDACTED>, Dustin Craig <REDACTED>,
cecilia.quiroz@phoenixcollege.edu, kerry.mitchell@domail.maricopa.edu,
tina.emmons@domail.maricopa.edu, Miguel Corzo <REDACTED>

Members of the Board,

Per MAT policy, we are now escalating the attached employee grievance to you, the MCCCD Governing Board.

Several members of ITS filed a critical grievance in October 2012 with the MCCCD Administration. This grievance has been escalated to all levels of management in the organization and we have not received a response to date.

Several letters (see attached) were sent to Dr.Glasper and Mr. Bowers by our MAT and PSA representatives requesting a response (see attached) and offering assistance.

At this time and a nearly a year and a half after this grievance was filed, nearly all warnings/issues raised in this grievance have now materialized at great financial costs to the institution. In addition, *nearly all ITS members who filed this grievance have either resigned, forced to retire or are facing disciplinary action up to an including termination.*

This grievance is significant because it is the official document that could have prevented many of the issues that have plagued the District for the last few years. It is now costing MCCCD millions of dollars to resolve these issues. Here is what this grievance was meant to prevent/address:

- The security breach of 2013 could have been prevented.
- The millions of dollars now spent with this breach could have been prevented.
- The millions of dollars wasted in failed BOND projects (CFS) mentioned in this grievance could have been saved.
- Lawsuits now filed against MCCCD could have been avoided.
- EEOC and other complaints regarding retaliation, mismanagement, abuse of authority, scapegoating and other matters could have been avoided.
- AZ Public Record laws and related financial penalties that MCCCD recently broke to protect itself could have been avoided.
- Management issues that led to spending millions in IT consultants could have been averted.
- Policy violations could have been avoided.
- The attrition of over 50% of the ITS department over the last 2 years could have been avoided.

- Millions to be spent on retraining and rehiring of IT employees could have been put to better use in the classroom.
- Millions to be spend on outsourcing of IT systems could have been directed towards hiring part time faculty.
- The damage to MCCCD reputation with our community could have been avoided.
- The impact to our future bond election is incalculable and yet to be determined.

*It is not too late. You must act NOW to address this grievance and save MCCCD from further financial damages. *

MCCCD employees paid a hefty price emotionally, personally and professionally when they filed this grievance to save MCCCD millions of dollars. We followed every process in place at MCCCD and we gave the Chancellor every opportunity to respond (18+ months). As you can see in the emails attached, Dr. Glasper, was encouraged multiple times to respond to this grievance. He indicated he would do so as recently as 1/2014 but he never did.

Per MAT policy, a response is due to employees who took a chance with their careers to bring matters of great importance to the attention of the MCCCD administration. You may contact Kerry Mitchell, Past MAT Executive President or Cecilia Quiroz, Past PSA President for additional details regarding this grievance.

The Chancellor's choice to ignore MAT policy and employee grievances have cost MCCCD millions of dollars and severely damaged its reputation in the community. We are now asking the MCCCD Governing Board to take these matters into their hands per MAT policy and Dr. Glasper's lack of response.

Here are the documents we are enclosing for your review:

13 - Original employee IT grievance filed in October 2012 (see page 4 for security warnings).

13b - Cover letter for IT grievance.

14a - Email sent to Dr. Glasper on 10/2012 by MAT and PSA Presidents bringing the grievance to his attention.

14b - Email from Dr. Glasper acknowledging his receipt of grievance.

15 - One of six emails sent by IT employees regarding this grievance and requesting that the grievance be addressed. This email cites financial risks to Maricopa if the grievance continues to be ignored.

16 - Response from Dr. Glasper to emails sent by employees.

29 - Response from Kerry Mitchell (MAT President) to more request from the grievants to please get a response from the Administration

34 - Yet another request sent by Kerry Mitchell to Dr. Glasper to please respond to the grievance.

36 - Yet another response from Dr. Glasper apologizing and stating that he will work on it with HR.

As you can see, we have given Dr. Glasper every opportunity to respond to this grievance. He never responded and MCCCD is now in a very dire situation.

*We request that the Governing Board hire an independent investigator to look into these matters. Furthermore, we are asking that the Board puts a hold on further disciplinary actions to ITS personnel until the issues on this grievance are addressed by the Board. *

Sincerely,

Miguel Corzo
Dustin Landagora
Christina Millanez
Earl Monsour
Gary Nusbaum