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

Submitted by

The Electronic Privacy Information Center

I. Introduction

1. This Complaint concerns Maricopa County Community College District's ("MCCCD," or "Maricopa" or "District") loss of personal data of almost 2,500,000 current and former students, employees, and vendors, following an earlier similar breach. As set forth in detail below, despite repeated warnings, the District failed to develop, implement, and maintain a comprehensive information security program. The District's failures led to a massive breach of names, dates of birth, addresses, phone numbers, e-mail addresses, Social Security numbers, demographical information, and enrollment, academic, and financial aid information.

2. As described below, MCCCD is a financial institution, engaged in the processing of financial transactions, subject to the Federal Trade Commission's Safeguards Rule. Maricopa's actions violated the Safeguards Rule.

3. Many educational institutions in the United States today are also subject to the Safeguards Rule. The MCCCD case is a particularly egregious example of the risk of failing to safeguard sensitive personal information.

4. The Electronic Privacy Information Center ("EPIC") submits this complaint as a supplement to a similar complaint filed by DataBreaches.net on June 14, 2014 (FTC Reference No. 54993134).

II. Parties

5. EPIC is a public interest research center located in Washington, D.C. EPIC focuses on emerging privacy and civil liberties issues and is a leading consumer advocate before the FTC. EPIC has a particular interest in protecting consumer privacy, and has played a leading role in developing the authority of the FTC to address emerging privacy issues and to safeguard the privacy rights of consumers.[1] EPIC has previously testified before Congress on the need for financial institutions and companies to protect consumers against data breaches.[2]

6. Maricopa County Community College District is a district comprised of ten colleges, two skill centers, and "numerous education centers" throughout Maricopa County in Arizona.[3]

III. Factual Background

A. The Maricopa County Community College District Maintains Nonpublic, Personal Information of Hundreds of Thousands of Students

7. Over 265,000 students attend Maricopa Community Colleges each year.[4]

8. The MCCCD provide students with financial assistance.[5]

---

[1] *See, e.g.*, Letter from EPIC Exec. Dir. Marc Rotenberg to FTC Comm'r Christine Varney (Dec. 14, 1995) (urging the FTC to investigate the misuse of personal information by the direct marketing industry), http://epic.org/privacy/internet/ftc/ftc_letter.html; DoubleClick, Inc., *FTC* File No. 071-0170 (2000) (Complaint and Request for Injunction, Request for Investigation and for Other Relief), http://epic.org/privacy/internet/ftc/DCLK_complaint.pdf; Microsoft Corporation, FTC File No. 012 3240 (2002) (Complaint and Request for Injunction, Request for Investigation and for Other Relief), http://epic.org/privacy/consumer/MS_complaint.pdf; Choicepoint, Inc., FTC File No. 052-3069 (2004) (Request for Investigation and for Other Relief) , http://epic.org/privacy/choicepoint/fcraltr12.16.04.html.

[2] *See*, *e.g.*, Testimony and Statement for the Record of Marc Rotenberg, Executive Director, Electronic Privacy Information Center on "Cybersecurity and Data Protection in the Financial Sector," Before the Senate Committee on Banking, Housing, and Urban Affairs, June 21, 2011, *available at* http://epic.org/privacy/testimony/EPIC_Senate_Banking_Testimony_20_6_21_11.pdf; Testimony and Statement for the Record of Marc Rotenberg, Executive Director, Electronic Privacy Information Center, Hearing on the Discussion Draft of H.R. ____, A Bill to Require Greater Protection for Sensitive Consumer Data and Timely Notification in Case of Breach, Before the House Committee on Energy and Commerce Subcommittee on Commerce, Manufacturing, and Trade, June 15, 2011, *available at http://epic.org/privacy/testimony/EPIC_Testimony_House_Commerce_6-11_Final.pdf. See also Identity Theft,* EPIC, http://epic.org/privacy/idtheft/.

[3] *About Us*, Maricopa Community Colleges, https://www2.maricopa.edu/about-us.

[4] *Demographics*, Maricopa Community Colleges, https://www2.maricopa.edu/about-us/quick-facts/demographics.

[5] *S-5 Student Financial Assistance*, Maricopa Community Colleges, http://www.maricopa.edu/publicstewardship/governance/adminregs/appendices/S-5.php.

9. MCCCD collects detailed, nonpublic personal information to facilitate student financial activities.

10. "New [MCCCD] students must complete" an application for federal financial aid, and "each academic year, continuing students must reapply" for federal financial aid.[6]

11. MCCCD requires certain students to undergo a verification process to facilitate their federal loan disbursement.[7]

12. In the verification process, students are required to provide Maricopa with personally identifiable financial information, including W-2s and salary information.[8]

13. After a student applies and is approved for federal financial aid, financial aid funds are dispersed and credited to student accounts to pay "current tuition, fees, and books."[9]

14. Maricopa then issues refunds for any remaining funds through the Maricopa Student Refund Program ("MSRP").[10]

15. Maricopa also issues book advances through the MSRP.[11] Maricopa issues book advances as pre-disbursements for student "anticipated financial aid" to be used for "education expenses [.]"[12]

16. Through the MSRP, Maricopa issues refunds to student accounts via "direct deposit, prepaid card, or paper check."[13]

17. To facilitate direct deposit, Maricopa obtains student bank account financial information.[14]

---

[6] *Id*.
[7] *Id*.
[8] *2013-2014 Verification Worksheet*, Maricopa Community Colleges, https://maricopa.service-now.com/sys_attachment.do?sys_id=c4b1a58d6f2d2100c85a6592be3ee447.
[9] *Reimbursement*, Maricopa Community Colleges, https://maricopa.service-now.com/student/knowledge.do?sysparm_document_key=kb_knowledge,dac9db536f952100ba08c951be3ee4f6&num=KB0010432&section=Finances.
[10] *Id*.
[11] *Book Advances*, Maricopa Community Colleges, https://maricopa.service-now.com/student/knowledge.do?sysparm_document_key=kb_knowledge,88d9b5416fdca100c85a6592be3ee485&num=KB0010176&section=Finances.
[12] *Id*.
[13] *Maricopa Student Refund Program (MSRP),* Maricopa Community Colleges, https://maricopa.service-now.com/student/knowledge.do?sysparm_document_key=kb_knowledge,8c4991016fe6a1004c7d6592be3ee4c4&num=KB0010476&section=Finances.
[14] *MSRP Enrollment Guide, page 7, https://maricopa.service-now.com/sys_attachment.do?sys_id=a094adef6f3e210009e28e354b3ee476.*

B. In 2011, MCCCD Disclosed Personal Information Without Obtaining Individual Consent

18. In January 2011, the Federal Bureau of Investigation informed Maricopa "one or more of MCCCD's databases were available for sale on the Internet."[15]

19. After being contacted by the FBI, MCCCD did not publically disclose to those impacted by the data breach the unauthorized sale of Maricopa databases.[16]

20. The MCCCD 2011 data breach affected 400 people.[17]

C. Following the 2011 breach, Arizona's Auditor General Recommended Changes in the Maricopa Information Security Program

21. In November 2011, the Arizona Auditor General issued a "Report on Internal Control and Compliance" that reviewed, among other things, Maricopa's computer information system's access and change controls.[18]

22. The Auditor General found that Maricopa "[u]sers' access rights [to Maricopa systems] were not always revoked after termination" and that "several terminated employees remained active system users more than 8 months after termination."[19]

23. The Auditor General also found that "[s]ystem activity was not monitored for those employees who had administrative and superuser access roles that granted them heightened user privileges."[20]

24. The Auditor noted that several Maricopa users "had the ability to make unauthorized changes to the District's systems."[21]

---

[15] Letter from Lori S. Nugent, Wilson Esler Moskowitz Edelman & Dicker, LLP, to N. C. Att'y Gen.'s Office, Consumer Prot. Div., 2 (Nov. 27, 2013), *available at* http://archive.azcentral.com/ic/pdf/0225mcc-data-breach.pdf.

[16] Mary Beth Faller, *Failure to Address 2011 Hacking Tied to '13 Breach*, ARIZONA REPUBLIC (Feb. 25, 2014), http://www.azcentral.com/community/phoenix/articles/20140318arizona-mcccd-failure-address-hacking-tied-breach.html.

[17] *Id*.

[18] Debra K. Davenport, State of Ariz. Office of the Auditor Gen., Fin. Audit Div., Report on Internal Control and Compliance: Maricopa County Community College District (2011), *available at* 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.

[19] *Id*. at 3.

[20] *Id*.

[21] *Id*.

25. The Auditor found that these "inadequate controls could lead to an increased risk of theft, manipulation, misuse of sensitive or confidential information by unauthorized users, or unauthorized changes or changes that were not made accurately."[22] The Auditor concluded that the inadequate controls and corresponding risks to information was "a material weakness in internal control over financial reporting."[23]

26. The Arizona Auditor also noted that Maricopa failed to implement the Auditor's earlier recommendations to correct computer access deficiencies.[24]

27. The Arizona Auditor General recommended that Maricopa strengthen Maricopa's computer access and change controls.[25]

28. In its Corrective Action Plan, Maricopa agreed with the Arizona Auditor's findings and claimed that the District would "address the issues identified" and monitor and review its information system "on a regular basis."[26]

D. In 2012, the Arizona's Auditor General Again Warned Maricopa of Vulnerabilities with the Maricopa Information Security Program

29. In November 2012, the Arizona Auditor General again found Maricopa did not adequately limit access to its information systems.[27]

30. The Auditor General found that Maricopa did not monitor all user access to Maricopa systems, and that Maricopa did not revoke "all terminated employees' access to its student information system [.]"[28]

31. The Auditor General noted that Maricopa failed to establish policies and procedures incorporating the Auditor's previous recommendations. [29]

32. The Auditor General recommended that the District "continue to strengthen computer access controls."[30]

---

[22] *Id*.
[23] *Id*.
[24] *Id*. at 3-4.
[25] *Id*. at 3.
[26] *Id*. at 6.
[27] Debra K. Davenport, State of Ariz. Office of the Auditor Gen., Fin. Audit Div., Report on Internal Control and Compliance: Maricopa County Community College District, 4 (2012), *available at* 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.
[28] *Id*.
[29] *Id*.
[30] *Id*.

33. In its Corrective Action Plan, the District agreed to implement procedures to strengthen computer access controls.[31]

E. In 2013, Maricopa Experienced a Second Data Breach that Disclosed Nonpublic Personal Information of Millions of Individuals

34. In April 2013, the FBI informed Maricopa of another breach affecting fourteen MCCCD databases.[32]

35. Specifically, the FBI informed MCCCD that fourteen MCCCD databases were listed for sale on a public website.[33]

36. The compromised databases included student "names, address, phone numbers, e-mail addresses, Social Security Numbers, dates of birth, certain demographical information, and enrollment, academic, and financial aid information."[34]

37. The breach affected 2.49 million current and former students, employees, and vendors.[35]

38. Maricopa began mailing breach notification letters in at the end of November 2013, approximately seven months after being notified of the breach.[36]

F. Following the 2013 Breach, a 2013 Arizona Auditor General Report Noted Vulnerabilities in Maricopa's Information Security Program

39. In December 2013, for the third year in a row, the Arizona Auditor General recommended that the District "strengthen its information system access and change controls."[37]

40. The Auditor General noted the 2013 breach, and that the District did not have adequate policies or procedures in place, as the Auditor General had noted in its 2012 Report. [38]

---

[31] *Id*. at 6.
[32] Letter from Lori S. Nugent, *supra* note 15.
[33] *Id*.
[34] *Id*. at 3.
[35] Tim Gallen and Mike Sunnucks, *Maricopa Community Colleges notifies 2.5M after data security breach*, PHOENIX BUS. J. (Nov 27, 2013), http://www.bizjournals.com/phoenix/news/2013/11/27/mcccd-notifies-25m-about-exposed.html?page=all.
[36] Letter from Lori S. Nugent, *supra* note 15, at 4; Cassie Klapp, *Student, worker data at risk at Maricopa colleges*, ABC 15 ARIZ. (Nov 27, 2013), http://www.abc15.com/news/region-southeast-valley/tempe/student-worker-data-at-risk-at-maricopa-colleges.
[37] Debra K. Davenport, State of Ariz. Office of the Auditor Gen., Fin. Audit Div., Report on Internal Control and Compliance: Maricopa County Community College District, 3 (2013), *available at* http://www.azauditor.gov/Reports/Community_Colleges/Maricopa_County_CC/Financial_Audits/IC_Control_and_Compliance_2013/Maricopa_CCCD_06_30_13_ROIC.pdf.
[38] *Id*. at 3-4.

IV. Legal Analysis

A. Maricopa County Community College District is a "Financial Institution" Subject to the "Safeguards Rule"

41. The Gramm-Leach-Bliley Act ("GLBA") "requires companies defined under the law as "financial institutions" to ensure the security and confidentiality of this type of information."[39]

42. The GLBA grants the FTC authority to conduct rulemaking in furtherance of the mandates of the Act.

43. In 2002, the FTC promulgated the "Safeguards Rule," which requires financial institutions under FTC jurisdiction to have measures in place to keep customer information secure.[40]

44. Under the GLBA, "financial institutions" subject to the FTC's jurisdiction for the purposes of the Safeguards Rule are "any institution the business of which is engaging in financial activities as described in section 4(k) of the Bank Holding Company Act of 1956 (12 U.S.C. 1843(k)). An institution that is significantly engaged in financial activities is a financial institution."[41]

45. Section 4(k) of the Bank Holding Company Act of 1956 (12 U.S.C. 1843(k)) in turn states that "lending, exchanging, transferring, investing for others, or safeguarding money or securities" are examples of activities "considered to be financial in nature."[42]

46. As described above, the Maricopa County Community College District is "lending, exchanging, transferring, investing for others, or safeguarding money or securities."[43] Specifically, MCCCD lends and transfers money to students through the Maricopa Student Refund Program. Maricopa is therefore a "financial institution" subject to the Safeguards Rule.

47. Institutions whose primary purpose is not finance can nevertheless be "financial institutions" under the Safeguards Rule.[44]

---

[39] Financial Institutions and Customer Information: Complying with the Safeguards Rule, Fed. Trade Comm'n, Bureau of Consumer Prot., http://www.business.ftc.gov/documents/bus54-financial-institutions-and-customer-information-complying-safeguards-rule.

[40] Standards for Safeguarding Customer Information, 67 Fed. Reg. 36484-01 (May 23, 2002) (codified at 16 C.F.R. § 314 et seq. (2014)).

[41] 16 C.F.R. § 313.3.

[42] 12 U.S.C. § 1843(k)(4)(a).

[43] 12 U.S.C. § 1843(k)(4)(a).

[44] The statute specifically contemplates the compliance of "instutions of higher education" at 16 C.F.R. § 313.1 (b) ("Any institution of higher education that complies with the Federal Educational Rights and

48. Under the Safeguards Rule, financial institutions are prohibited from disclosing "non-public personal information" to "nonaffiliated third parties" unless they notify consumers of their right to opt-out of the disclosure. [45]

49. "Nonpublic personal information" is "personally identifiable financial information; and any list, description, or other grouping of consumers (and publicly available information pertaining to them) that is derived using any personally identifiable financial information that is not publicly available."[46]

50. Personally identifiable financial information is "any information: (i) A consumer provides . . .to obtain a financial product or service from [a financial institution]; (ii) About a consumer resulting from any transaction involving a financial product or service between [a financial institution] and a consumer; or (iii) [a financial institution] otherwise obtain[s] about a consumer in connection with providing a financial product or service to that consumer."[47]

51. Personally identifiable financial information includes information provided to a financial institution "on an application to obtain a loan, credit card, or other financial product or serve."[48]

52. In addition to prohibiting financial institutions from disclosing "non-public personal information to nonaffiliated third parties," the Safeguards Rule obligates financial institutions "develop, implement, and maintain a comprehensive information security program."[49]

53. The program must contain "administrative, technical, and physical safeguards that are appropriate" for the size and complexity of the financial institution in question, given the nature and scope of the institution's activities, and the "sensitivity of any customer information at issue."[50]

54. More specifically, in developing, implementing, and maintaining the information security program, financial institutions must "designate an employee or employees to coordinate [the] information security program."[51]

Privacy Act…and that is also a financial institution subject to the requirements of this part, shall be deemed to be in compliance with this part if it is in compliance with FERPA").

[45] 16 C.F.R. § 313.10.
[46] 16 C.F.R. § 313.3 (n)(1).
[47] 16 C.F.R. § 313.3(o) (1).
[48] 16 C.F.R. § 313.3(o) (2)(i)(A).
[49] 16 C.F.R. § 314.3.
[50] 16 C.F.R. § 314.3.
[51] 16 C.F.R. § 314.4.

55. Further, they must "identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that could result in the unauthorized disclosure, misuse, alteration, destruction or other compromise of such information, and assess the sufficiency of any safeguards in place to control these risks. At a minimum, such a risk assessment should include consideration of risks in each relevant area of your operations, including: (1) Employee training and management; (2) Information systems, including network and software design, as well as information processing, storage, transmission and disposal; and (3) Detecting, preventing and responding to attacks, intrusions, or other systems failures."[52]

56. They must "design and implement information safeguards to control the risks [the financial institution identifies] through risk assessment, and regularly test or otherwise monitor the effectiveness of the safeguards' key controls, systems, and procedures."[53]

57. Additionally, they must "oversee service providers, by: (1) Taking reasonable steps to select and retain service providers that are capable of maintaining appropriate safeguards for the customer information at issue; and (2) Requiring [the financial institution's] service providers by contract to implement and maintain such safeguards."

58. Finally, these financial institutions are required to "evaluate and adjust [their] information security program[s] in light of the results of the testing and monitoring required by [the Rule]."[54]

59. The Safeguards Rule also specifies that the FTC has enforcement authority under the Federal Trade Commission Act, 15 U.S.C.A. § 41 et seq."[55]

60. As described above, the Maricopa County Community College District disclosed non-public personal information to nonaffiliated third parties.

61. Maricopa County Community College District also failed to develop, implement, and maintain a comprehensive information security program appropriate for the sensitivity of its activities.

B. Count I: Disclosure of Non-public Personal Information to Nonaffiliated Third Parties

62. As described above, the Maricopa County Community College District is subject to the Safeguards Rule.

[52] 16 C.F.R. § 314.4.
[53] 16 C.F.R. § 314.4.
[54] 16 C.F.R. § 314.4.
[55] 15 U.S.C. § 6805(a)(7).

63. Because it is subject to the Safeguards Rule, Maricopa is prohibited from disclosing "any nonpublic personal information about a consumer to a nonaffiliated third party" unless Maricopa notifies consumers of their rights to opt-out of the disclosure.

64. In the 2013 breach, Maricopa disclosed non-public personal information when it disclosed personally identifiable financial information of Maricopa students, employees, and vendors.

65. Maricopa's unauthorized disclosure of non-public personal information violated 16 C.F.R. § 313.10.

C. Count II: Failure to Conduct Testing and Monitoring in Violation of Safeguards Rule

66. As described above, despite Maricopa's repeated representations to the Arizona Auditor General, Maricopa did not test and monitor its information security program.

67. Therefore, Maricopa's failure to test and monitor its information security program constitutes a violation of 16 U.S.C. § 313.3.

D. Count III: Failure to Adjust Information Security Programs in Violation of Safeguards Rule

68. Because Maricopa did not conduct testing and monitoring as required by the Safeguards Rule, Maricopa did not adjust its information security programs following the 2011 information security breach.

V. Prayer for Investigation and Relief

69. EPIC urges the Commission to investigate Maricopa County Community College District and enjoin its failure to safeguard students' financial data.

70. Specifically, EPIC requests the Commission to:

    a. Examine the practices of the Maricopa County Community College District to evaluate whether they comply with the Safeguards Rule;

    b. Require the Maricopa County Community College District, in connection with its compliance with the Safeguards Rule, to obtain an assessment and report from a qualified, objective, independent third-party professional to insure that it is complying with the Safeguards Rule; and

c. Bring an enforcement action in federal district court for violation of the Safeguards Rule.

d. Examine the practices of other similar educational institutions, providing financial services, whose failure to follow the Safeguards Rule may have placed at risk the personal financial information of students.

Respectfully Submitted,

Marc Rotenberg, EPIC Executive Director
Khaliah Barnes, Director, EPIC Student Privacy Project
Julia Horwitz, EPIC Consumer Protection Counsel
Brett Weinstein, EPIC Extern
Sara Bennett, EPIC Extern
Electronic Privacy Information Center
1718 Connecticut Ave. NW Suite 200
Washington, DC 20009
202-483-1140 (tel)
202-483-1248 (fax)