VIA ELECTRONIC SUBMISSION: https://ftcpublic.commentworks.com/ftc/safeguardsrulenprm/

November 3, 2016

Federal Trade Commission
Office of the Secretary
600 Pennsylvania Avenue N.W.
Suite CC-5610 (Annex B)
Washington, D.C. 20580

Re: Request for Public Comment on "Standards for Safeguarding Customer Information" (Safeguards Rule, 16 CFR 314, Project No. P145407), September 7, 2016

To Whom It May Concern:

EDUCAUSE and the National Association of College and University Business Officers (NACUBO) respectfully submit these comments to the Federal Trade Commission (FTC) in response to the above-referenced request for comments (RFC) published in the *Federal Register* on September 7, 2016, at 16 CFR 314. Our comments pertain to Section III.B, "Specific Issues," Questions 1, 2, and 3, and Section III.A, "General Issues," Question 12.

EDUCAUSE (www.educause.edu) is a non-profit association and the foremost community of information technology (IT) leaders and professionals committed to advancing higher education. Our membership includes over 2,000 colleges and universities, over 350 corporations serving higher education IT, and dozens of other associations, state and federal agencies, college and university system offices, and not-for-profit organizations. EDUCAUSE strives to support IT professionals and the further advancement of IT in higher education through analysis, advocacy, community- and network-building, professional development, and knowledge creation.

NACUBO (www.nacubo.org) represents more than 2,500 colleges, universities, and higher education providers. It represents chief business and financial officers through advocacy efforts, community service, and professional development activities. NACUBO's mission is to advance the economic viability and business practices of higher education institutions, including in the IT space, to support the fulfillment of their academic missions.

Higher education institutions occupy a unique space under the Gramm-Leach-Bliley Act (GLBA). While GLBA ostensibly focuses on entities engaged in banking and financial services, the role of colleges and universities in supporting financial aid access for students places them within the scope of the Privacy and Safeguards Rules established under GLBA. In implementing the Privacy Rule, the FTC recognized higher education institutions' preexisting, substantive obligations for the privacy of student records under the Family Educational Rights and Privacy Act (FERPA) and equated Privacy Rule compliance with FERPA compliance. Institutions remain accountable for Safeguards Rule compliance directly, however, along with other covered entities.

As a result, EDUCAUSE and NACUBO members maintain a vital interest in FTC efforts to update the Safeguards Rule. We appreciate the opportunity to offer input into that process and ask the Commission to consider our comments on the following questions. We answer each question briefly in order of priority and then explain our thinking about the questions as a set in more detail.

- *(Section III.B, "Specific Issues," Questions 2) Should the Rule be modified to include more specific and prescriptive requirements for information security plans? Why or why not? If so, what requirements should be included and what sources should they be drawn from?*

  No, the FTC should preserve the Rule's flexibility, which allows an organization to develop a security plan that fits its unique context based on the standard(s) that best apply to it. In providing guidance, the FTC might clarify the importance of standards-based approaches and how organizations can best illustrate the fit between their contexts and the standards and plans they adopt. Imposing specific requirements, though, would shift the organization's focus from what works in its world to regulatory compliance.

- *(Section III.B, "Specific Issues," Questions 3) Should the Rule be modified to reference or incorporate any other information security standards or frameworks, such as the National Institute of Standards and Technology's Cybersecurity Framework or the Payment Card Industry Data Security Standards? If so, which standards should be incorporated or referenced and how should they by referenced or incorporated by the Rule?*

  No, incorporating a specific standard or framework in the Rule would impose a "one-size-fits-all" approach that undermines the Rule's inherent flexibility in relation to the issues it covers. Specifying a particular standard or framework would also add a layer of complexity to an already complex environment in which institutions must integrate numerous preexisting federal and state requirements. The cumulative effect would be to undermine compliance and cybersecurity success in a very diverse higher education sector, where institutions can differ greatly in both size and available resources.

- *(Section III.B, "Specific Issues," Questions 1) Should the elements of an information security program include a response plan in the event of a breach that affects the security, integrity, or confidentiality of customer information? Why or why not? If so, what should such a plan contain?*

  No, the standards or frameworks that organizations adopt to fit their context would address their breach response needs, consistent with the current requirement for incident response planning. Maintaining context-based standards and plans is important given the many federal and state breach requirements institutions already face.

- *(Section III.A, "General Issues," Question 12) Does the Rule overlap or conflict with other federal, state, or local laws or regulations? If so, how?*

  If the FTC alters the Rule to incorporate specific standards or frameworks, it likely would generate overlap or conflicts with other laws and regulations as previously mentioned.

Analysis:

Colleges and universities serve as examples that validate a core principle of the Safeguards Rule: the information security plans and practices of affected organizations should be governed by what is "appropriate to the size and complexity of the financial institution, the nature and scope of its activities, and the sensitivity of any customer information at issue."[1] Higher education institutions are incredibly diverse, encompassing a wide variety of missions, operations, and student populations. They may hold roughly similar data related to student financial aid, but that data forms only part of the security environment they must manage.

Colleges and universities focus on risk-based, integrated approaches to defining and deploying appropriate safeguards. This allows them to account for the full range of information they must secure and requirements they must meet (e.g., HIPAA/HITECH, FISMA, state information security and breach notification laws, PCI DSS, federal export controls such as EAR and ITAR). Their approaches are generally standards-based, reflecting well-established national and international information security frameworks. (See, for example, the EDUCAUSE Higher Education Information Security Council's *Information Security Guide: Effective Practices and Solutions for Higher Education.*[2])

Higher education institutions rely on the flexibility of the Safeguards Rule to craft information security programs that draw on the framework(s) most relevant to their missions, operations, and the data those entail. The mission and operations of a community college generate information security requirements distinct from those of a liberal arts college, a comprehensive state university, or a research-intensive university. How each institution designs its information security program should reflect the totality of its unique needs and related risk assessments, which includes the numerous federal and state information security standards it already faces.

Introducing rigidity into a previously flexible Safeguards Rule has the potential to distort information security planning and practice. For example, it may easily lead to merely documenting regulatory compliance over instituting risk-based controls appropriate for the institution given what it does, who it serves, and the risks associated with the underlying data to be protected. If this occurs, very limited resources would likely be diverted to sub-optimal activities. Implementing controls strictly because of regulations could leave begging those processes and practices truly driven by an objective assessment of risk. This would degrade the effectiveness of the institution's approach to information security and ultimately undermine the protection of the type of customer information the Rule is intended to safeguard.

As the FTC considers changes to the Rule, it may make sense to also consider how best to discuss the importance of standards-based approaches to information security in the related guidance that the Commission provides. Likewise, the commission might choose to update such guidance to include recommendations on how affected organizations can most effectively illustrate the connections between their size, complexity, activities, et cetera, and the security standards and plans they have adopted. However, incorporating further specifications for information security plans into the Rule, possibly including the particular standards framework(s) with which plans must comply, could quickly prove counter-productive since one size does not fit all when it comes to higher education. For example, a research-intensive university may choose to implement security controls relevant to its research

[1] 16 CFR 314.3(a).

[2] https://library.educause.edu/resources/2014/5/information-security-guide-effective-practices-and-solutions-for-higher-education

function. This would make sense given the information security needs and requirements various forms of grant-funded research might entail. Forcing institutions with little-to-no externally funded research to adopt such controls, however, would impose a heavy, unnecessary burden, both fiscally and operationally. They simply would not have the staff and resources to implement the same security measures as their research counterparts, nor the operations and risks to justify it.

On the issue of breach response, a specific reference to it in the Safeguards Rule is unnecessary and, at least for higher education, potentially counter-productive. Breach response is a standard feature of incident response planning addressed by almost every information security standard and set of reasonable practices. The Safeguards Rule's existing requirement for comprehensive security plans to address "detecting, preventing and responding to attacks, intrusions, or other systems failures"[3] already encompasses it. Specifying a breach requirement in the Rule, separate and apart from incident response, may only serve to create confusion for higher education institutions by introducing one more factor to the already complex analysis of current federal and state mandates that institutions must execute during a breach.

The Commission and Safeguards Rule stakeholders would be better served if the FTC aggregated and promoted public resources highlighting widely accepted security frameworks across a range of organizational types and information security needs. As part of this effort, the FTC could specifically note the consistency of breach notification as a feature of incident response requirements, along with common principles and effective practices. This would encourage both greater Safeguards Rule compliance and continuous improvement in information security.

EDUCAUSE, NACUBO, and their members would be happy to work with the FTC and other stakeholders to inform such an effort. In the interim, thank you for the opportunity to contribute to this important process.

Sincerely,

Jarret S. Cummings
Director
Policy and Government Relations
EDUCAUSE

Elizabeth L. Clark
Director
Federal Affairs
NACUBO

[3] 16 CFR 314.4(b)(3).