American Council on Education®
One Dupont Circle NW
Washington, DC 20036
(202) 939-9300
acenet.edu

August 2, 2019

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 Notice of Proposed Rule-Making, "Standards for Safeguarding Customer Information" (Safeguards Rule, 16 CFR 314, Project No. P145407), August 2, 2019

To Whom It May Concern:

On behalf of the associations listed below, representing college leaders, educators, and professionals, we write offering comments to the Federal Trade Commission (FTC) regarding the above-referenced notice of proposed rule-making (NPRM) concerning 16 CFR 314, "Standards for Safeguarding Customer Information" (hereafter referred to as "the Safeguards Rule" or "the Rule"), published in the Federal Register on April 4, 2019, at:

https://www.federalregister.gov/documents/2019/04/04/2019-04981/standards-for-safeguarding-customer-information#addresses

Two of the undersigned associations (EDUCAUSE and the National Association of College and University Business Officers) offered comments during the Commission's 2016 process on potential updates to the Safeguards Rule.[1] We are pleased that the FTC considered some of the points raised in that submission, as indicated by the references to those previous comments in the NPRM.

We would reiterate the concerns raised in those prior comments about the potential for the FTC to deviate from its long-standing, flexible approach to information security program development and implementation. The current text of the Rule clearly reflects that flexibility, consistent with the principles inherent in its underlying legislation, the Gramm-Leach-Bliley Act (GLBA). As Commissioners Phillips and Wilson noted in their dissent[2] regarding the NPRM, though, the Commission's proposed changes to the Safeguards Rule reflect a significant departure from its historical emphasis on discretion for covered entities in fulfilling the Rule's requirements.

---

[1] EDUCAUSE and NACUBO, Comments on "Request for Public Comment, 'Standards for Safeguarding Customer Information' (Safeguards Rule, 16 CFR 314, Project No. P145407), September 7, 2016," November 3, 2016 (https://library.educause.edu/resources/2016/11/educause-comments-glba-safeguards-rule).

[2] Noah Joshua Phillips and Christine S. Wilson, "Dissenting Statement of Commissioner Noah Joshua Phillips and Commissioner Christine S. Wilson - Regulatory Review of Safeguards Rule," Federal Trade Commission, March 5, 2019 (https://www.ftc.gov/public-statements/2019/03/regulatory-review-safeguards-rule-dissenting-statement-commissioner-noah).

Such a significant departure poses major challenges for colleges and universities of all types, with many if not most likely to find those challenges insurmountable within the proposed compliance timeframe. This consideration arises even before one discusses whether many of the Commission's proposals are appropriate to the size and complexity of colleges and universities, much less to the nature and scope of the activities that lead them to be covered by the Rule. With that in mind, we first note a few general concerns with the Commission's approach and then discuss specific points and recommendations related to the proposal's individual provisions.

General Concerns

1. *Colleges and universities may technically be considered "financial institutions" under the Safeguards Rule, but we are fundamentally academic institutions. The current Rule's flexible approach allows us to bridge those realities. The proposed new Rule highlights where they diverge and has the potential to make Rule compliance—not the college or university's academic mission or its assessment of risk in relation to that mission—the basis of its information security program.*

   The FTC determined over 15 years ago that the role played by colleges and universities in facilitating student access to loans and other relevant forms of financial aid placed them under the definition of "financial institution" as established in the Gramm-Leach-Bliley Act (GLBA) by reference to the Bank Holding Company Act of 1956. The term only applies in a technical sense, however, and the replacement of the guaranteed student loan program with the federal direct student loan program in 2010 as well as the end of the Perkins Loan Program in 2017 have made that even more the case.

   Assisting students and their families in assembling the financial means for students to pursue higher education is a vitally important function at colleges and universities led by highly qualified, dedicated professionals. It is not, however, the basis on which the institution, its operations, and its technical infrastructure are organized. Colleges and universities have as their mission the expansion, preservation, transmission, and application of knowledge through research, education, and service. These inherently collaborative activities produce IT environments that necessarily involve a high degree of openness, decentralization, and diversity of systems and functions. Higher education institutions therefore must manage the security of the "customer information" related to the provision of student financial aid services—the Rule's primary concern in our context—via information security programs that have to account for a much broader range of data needs and requirements than those of typical financial services operations.

   The flexibility inherent in the current Rule allows colleges and universities, as well as the FTC itself, to balance those basic distinctions. The existing elements of the Rule establish an outline for a compliant information security program that allows institutions to set the details of program leadership, risk assessment, safeguards development, and vendor oversight in ways that are specific to the Rule when necessary, but consistent with the reality of what higher education institutions actually *do* as appropriate.

   The Rule's emphasis on institutional discretion in meeting a broad but limited set of requirements for developing and implementing information security programs "appropriate to your size and complexity, the nature and scope of your activities, and the sensitivity of any customer information at issue"[3]—text which is also in the proposed revised Rule—allows colleges and universities to address their compliance responsibilities as "financial institutions" under the Rule within the context of their broader academic missions. By imposing many new, detailed requirements for Rule-compliant information security

[3] 16 CFR 314.3(a).

programs—even in the absence of delineating all of the standards and provisions with which they must align—the Commission now proposes to largely define the structure of information security at colleges and universities primarily in relation to "customer information" ahead of the many other mission-driven needs and requirements their information security programs must address. This would lead to the imposition of security requirements on research, learning, and service activities that may not be appropriate and could frustrate the purposes they are intended to achieve while adding greatly to the complexity and cost of the institution's overall information security.

For example, continuous monitoring of authorized users in relation to administrative functions may or may not be necessary in the context of securing "customer information." We would argue that individual institutions should make that determination based on risk assessments driven by their size and complexity, the nature and scope of their activities, and so forth. However, a Rule provision of this type that is not carefully and specifically scoped to address the "customer information" the Rule is intended to cover may lead higher education institutions to conclude that they have to extend continuous monitoring of authorized users across their IT environments. This would rightfully raise concerns about academic freedom and free speech among faculty and students, and thus inhibit teaching, learning, and research. It would also greatly increase the financial, technical, and staff resources necessary to implement and maintain such activity, detracting from the institution's capacity to support its mission-critical programs and services. And in the end, it would do little to enhance the security of personal financial information, which is the Rule's purpose.

2. *Specifying the elements and requirements of a Rule-compliant information security program to the degree proposed in the revised Rule creates substantial new compliance burdens on colleges and universities as well as guidance responsibilities for the FTC.*

The previous example is but one of many that we illustrate in relation to sections of the proposed revised Rule below. Collectively, the section-by-section points we raise demonstrate that the FTC's effort to balance many specific new requirements while preserving some degree of flexibility for covered entities ultimately proves to be problematic. The current Rule leaves the relevant issues in the hands of the covered entity subject to broad requirements for program leadership, risk assessment, safeguards development, and vendor oversight. The proposed revised Rule, however, specifies many of the details of those elements while adding more provisions and requirements, but without providing effective guideposts for compliance. That leaves colleges and universities with many questions about whether the proposed Rule's provisions are appropriately limited to the data and functions it covers and how institutions will effectively be able to determine if they are in compliance regardless.

We do not suggest, however, that the Commission should seek to delineate particular standards that covered entities must follow, particular technologies and applications they must adopt, and so forth. Given the concerns that colleges and universities have about the potential misalignment between the detailed provisions in the proposed revised Rule and our missions, operations, and IT environments, it seems likely that additional, more detailed specifications would only further limit the institutional discretion necessary to make the Rule work in the higher education context. So, while we share the FTC's goal of continuing to improve the security of relevant data, we believe a better approach to achieving it would be to maintain the current Rule and enhance guidance and effective practices dissemination around it, as EDUCAUSE and NACUBO called for in their 2016 comments. In the absence of that, we would urge the FTC to explicitly state in the Rule and subsequent guidance what we believe the proposed revised Rule implies—that institutions may achieve compliance through providing reasonable explanations in their information security program documentation for the choices they make in fulfilling the given provisions.

Furthermore, the new Rule should explicitly state that the Commission will seek to resolve any concerns it may have about an institution's exercise of discretion in fulfilling a given provision first through dialogue with the institution and the institution's subsequent demonstration of voluntary compliance, as compared to formal action. Finally, the FTC should greatly expand the resources and information it makes available to covered entities—as well as its collection of the same from them—about what one might generally consider to be effective policies, procedures, and practices in relation to the Rule and its application. To the extent these recommendations do not align with the Commission's established enforcement model, we would again propose that it maintain the Rule in a fashion that does not create the compliance confusion we discuss below.

3. *The proposed revised Rule does not clearly account for the ongoing, and accelerating, trend toward the use of third-party cloud services to meet relevant data processing and storage as well as customer service needs. The Commission should clarify the extent to which key compliance issues can appropriately be addressed in the context of such services prior to publishing a revised Rule.*

Colleges and universities increasingly rely on enterprise systems and data storage/management services provided by cloud vendors, meaning that they contract with third-party providers for access to and support of relevant functions via software and storage hosted remotely and made available over broadband networks. For example, of the approximately 500 U.S. higher education institutions that completed the relevant section of the EDUCAUSE Core Data Service 2018 Survey, 97% used the cloud for at least 5 information systems, and there was a 3% increase from FY17 to FY18 in the average number of core information systems that U.S colleges and universities sourced from the cloud.[4]

Cloud services often include features that enhance information security consistent with the intent of the proposed revised Rule, such as data encryption, and many higher education institutions, especially small- and medium-sized ones, consider cloud services as a primary path to accessing and maintaining industry-standard security for their enterprise systems and data. Some of the revised Rule's requirements as currently written do not take into account the limitations that often exist on institutional access to service provider infrastructure and operating processes, however, and thus those provisions do not provide a clear path for compliance via cloud services. The proposed 314.4(f) establishes institutional responsibility for vendor oversight in relation to the institution's information security program, but as we discuss below, the Commission may need to add cloud-specific provisions to certain requirements to harmonize those requirements with 314.4(f) as it relates to cloud services providers.

Proposed New Safeguards Rule Requirements and Provisions

In reviewing the specific proposals for a revised Safeguards Rule, the higher education community identified a number of points or questions about various provisions that we would like to call to the Commission's attention for clarification or action.

16 CFR 314.5, Effective Date (Allow two years for institutions to achieve compliance, with a one-year deadline for developing a plan to do so)

We urge the Commission to reconsider making numerous proposed additions or changes to the Safeguards Rule effective six months from the final Rule's publication date. Few colleges and universities are likely to have all of

[4] EDUCAUSE Core Data Service dataset as of July 1, 2019: www.educause.edu/research-and-publications/research/core-data-service.

the proposed new elements and requirements in place or in progress at the time of the final Rule's publication. The vast majority will need to implement some or several new security program elements and six months simply will not allow sufficient time to plan, budget, and operationalize those new requirements. We therefore propose that *institutions have one year to produce a comprehensive plan for achieving compliance with the final Rule,* assuming that it will likely include at least a significant number of the proposed new requirements, *and a subsequent year to fully implement that plan*, such that institutions would be in compliance within two years from the effective date of the final Rule.

As public and private, nonprofit colleges and universities, our member institutions generally operate under tight fiscal constraints, with limited capacity to absorb significant expenses occurring outside the normal budget cycle. An institution with a risk assessment that doesn't substantially conform to the new requirements of the proposed 314.4(b)(1) would have to initiate a process to replace or significantly revise its existing one. The financial and operational resources involved in that effort would be considerable. If the institution has to be sure that the process starts and finishes in time to have any resulting changes to its information security program largely operational within the same six-month window, the financial and resource implications would likely increase dramatically. For example, if the institution doesn't already have multi-factor authentication (MFA) and end-to-end as well as at-rest encryption in place on all networks and systems relevant to customer information, absorbing unplanned, unbudgeted application, staffing, and consulting costs for acquisition and implementation—within the compressed timeframe the Commission proposes—would likely be a major concern.

The same holds true for any combination of the proposed new elements of the Safeguards Rule that would have to be in place six months from the revised Rule's effective date per 314.5, including continuous monitoring or annual penetration testing/biannual vulnerability assessment, information security personnel policy changes under 314.4(a) and (e), secure development and/or security testing procedures for any applications related to the handling and processing of customer information, and so forth. Again, any one of these steps might be a challenge in a six-month window—an institution that must address many or all of them to some degree simply might not be able to comply in that timeframe.

16 CFR 314.6, Exceptions (Adopt a threshold for exempting small colleges and universities based on Carnegie Classification)

In relation to the proposed exceptions under 314.6, which the Commission would apply to covered entities that maintain relevant information on fewer than 5,000 consumers, we recommend that the FTC consider a different threshold for colleges and universities. Simply put, the 5,000-consumer metric does not appropriately account for the difference between actual financial services or relevant commercial entities and higher education institutions. An institution's Carnegie Classification, which is based on its number of full-time enrolled students, is a much more relevant measure of college and university size and therefore capacity to address the FTC's proposals:

> Colleges and universities use the Carnegie Classifications (http://carnegieclassifications.iu.edu/) as universal identifiers of institutional demographics. Those classifications define institutional size based on a calculation called Full Time Enrollment (FTE), which incorporates the number of students enrolled full-time and part time at an institution for an accurate gauge of an institution's relative size. This is a long-standing measure that is well-understood within higher education.[5]

[5] ACE, et al, Comments on "Supplemental Advance Notice of Proposed Rulemaking (SANPRM) relating to Nondiscrimination on the Basis of Disability; Accessibility of Web Information and Services of State and Local Government Entities and Public

Under the Carnegie Classification system, two-year postsecondary institutions with 2,000 or fewer FTE would be classified as "small," while four-year postsecondary institutions with 3,000 or fewer FTE would fall into the "small" category.[6] Even though such institutions enroll many fewer than 5,000 "consumers" during any relevant period, they might easily have "customer information" (i.e., student records) in excess of that threshold given record-retention requirements under other federal and state laws or regulations, or institutional policies to serve alumni. Thus, they would not qualify for the proposed exceptions as 314.6 is currently written.

The capacity of such institutions to meet the requirements identified under 314.6, though, would be based on institutional resources tied to their student population size, which provides a rough analogue to the resources that a small company or firm with 5,000 or fewer customers might have. Since the relevant measure for colleges and universities of institutional capacity to meet the FTC's proposed new requirements is Carnegie Classification based on FTE, we urge the Commission to apply the exceptions proposed under 314.6 to colleges and universities classified as "small" on that basis.

16 CFR 314.2(c), Definition of "Security Event" (Exempt encrypted data, distinguish between incidents and substantive "security events," and add "substantial harm or inconvenience" as a defining criterion)

The discussion in the NPRM of the definition of "security event" under the proposed revised Rule notes that the Commission omitted from it the exemption for "the acquisition of encrypted information" that was in the original "security event" definition from which the FTC's definition is drawn.[7] We would argue that the FTC should include the exemption for the acquisition of encrypted information in its "security event" definition. The FTC cites as the basis for this exclusion the view that the acquisition of encrypted information, even if the encryption key is not compromised, should still trigger action under a covered entity's incident response plan mandated by the proposed 314.4(h).[8] However, per the version of the definition that the Commission proposes to adopt, encrypted information where the encryption key has not been compromised cannot reasonably be said to have undergone unauthorized access or misuse, and if its acquisition does ultimately lead to an information system disruption, it would fall under the FTC definition of "security event" in any case.

Furthermore, the Commission's rationale for its initial decision might better be served by *clearly distinguishing between an incident and a "security event."* Institutions deploy operational policies and procedures to regularly thwart attempts to compromise the security of their networks, systems, and data; as a result, such incidents fail to rise to the level of a "security event" requiring a broad, institutional response. With that in mind, exempting the acquisition of encrypted data from the definition of a "security event" would make sense, knowing that an institution's ongoing information security operations encompass the handling of incidents that do not, for example, constitute a data breach and therefore would not trigger a breach response.

In addition, clearly delineating the distinction between an incident and a "security event," which may mean further modifying the proposed "security event" definition, would help covered entities to avoid confusion about what does and does not meet the "unauthorized access, disruption, or misuse" standard in the FTC's

---

Accommodations, 81 Fed. Reg. 28,658 (May 9, 2016),"p. 10: https://library.educause.edu/-/media/files/library/2016/10/highereddojsanprmcomments.pdf.

[6] Ibid.

[7] Federal Trade Commission, "Standards for Safeguarding Customer Information (Safeguards Rule), 16 CFR Part 314" (Notice of Proposed Rulemaking), *Federal Register*, Vol. 84, No. 65, April 4, 2019, p. 13164 (https://www.federalregister.gov/documents/2019/04/04/2019-04981/standards-for-safeguarding-customer-information#addresses).

[8] Ibid.

"security event" definition. As the definition currently stands, the accidental, and therefore unauthorized, deletion of a single record might possibly be seen as a "security event," even though the incident would not qualify as such under any common sense understanding of the term.

This is where the Commission should consider incorporating into its definition of "security event" the text from 314.3(b)(3), "unauthorized access to or use of such information that *could result in substantial harm or inconvenience to any customer*" (emphasis added), to set a clear, appropriate standard for determining if an incident truly rises to the level of a "security event." Such a revision to the proposed definition would be consistent, for example, with the "Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice,"[9] which was adopted by several federal financial agencies in relation to their GLBA privacy and security oversight responsibilities.

16 CFR 314.2(d), Definition of "Customer Information" (Include the Privacy Rule terms and definitions relevant to understanding what constitutes "customer information" in the revised Safeguards Rule)

The Commission notes in the NPRM that it proposes to incorporate the full definition and set of examples for "financial institution" (314.2(f)) from the Privacy Rule into the Safeguards Rule to facilitate greater understanding by covered entities of their status as "financial institutions." We would encourage the Commission to do the same with the definition of "customer information" as presented in 314.2(d). Rather than relying on the current reference to the Privacy Rule to direct attention to the range of terms that inform the "customer information" definition, we recommend that the FTC include a number of Privacy Rule definitions under 314.2(d) or under 314.2 generally. That would make it easier for covered entities to follow the interrelated chain of terms that defines the scope of the "customer information" they must secure under the revised Rule. The relevant definitions are:

- 16 CFR 313.3(e), "Consumer"
- 16 CFR 313.3(h), "Customer"
- 16 CFR 313.3(i), "Customer Relationship"
- 16 CFR 313.3(n), "Nonpublic Personal Information"
- 16 CFR 313.3(o), "Personally Identifiable Financial Information"
- 16 CFR 313.3(p), "Publicly Available Information"

16 CFR 314.2(e), Definition of "Encryption" (Rephrase to make "industry standards" a key criterion)

The proposed definition of "encryption" is too vague to provide an appropriate level of assurance for institutions regarding compliance. The Commission might consider rephrasing the definition in terms of "the transformation of data in accordance with industry standards to minimize the probability of assigning meaning…" That would provide covered entities with a basis for establishing the validity of the encryption approaches they utilize per the proposed requirements of the revised Rule.

16 CFR 314.2(h), Definition of "Information System" (Revise to clearly focus solely on the data and systems specifically related to the handling and management of "customer information")

[9] "Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice," *Federal Register*, Vol. 70, No. 59, March 29, 2005; see "A. Standard for Providing Notice," p. 15752 (https://www.gpo.gov/fdsys/pkg/FR-2005-03-29/pdf/05-5980.pdf).

The Commission's proposed definition of "information system" extends well beyond any industry-standard understanding of the term and would essentially place it in the position of overseeing virtually all aspects of institutional information security. This takes the Commission well beyond the legislative mandate established in GLBA that provides the fundamental basis for the Rule. The definition's proposed inclusion of "any specialized system such as industrial/process controls systems, telephone switching and private branch exchange systems, and environmental controls systems" appears intended to address, for example, possible Internet of Things (IoT) security issues that might allow a malign actor to compromise networks and systems that might conceivably allow such an actor to reach systems and data stores that actually pertain to "customer information."

However, under this thinking, the Commission would essentially be asserting oversight of any aspect of an institution's IT infrastructure that connects with the Internet, regardless of whether it is actually involved in the processing and handling of data related to the financial services consumers on which GLBA focuses. For example, even if a college or university "air gapped" the systems and databases it utilizes to handle student financial aid data—however unlikely and cost-prohibitive—the proposed definition could still be read as giving the Commission jurisdiction over information security planning for the institution as a whole, despite the segregation of the institution's "customer information" data and systems from Internet access.

In short, from a higher education perspective, this definition places the FTC on an extremely slippery slope given the diverse, decentralized networking and systems infrastructures and data stores our institutions utilize to align with and support the diverse, multi-faceted elements of our research, learning, and service missions, where other federal and state compliance claims may come into play. We strongly urge the Commission to redraft this definition, focusing on the technical resources and databases that directly pertain to the "customer information" at issue under GLBA. The FTC should take this step in the knowledge that Rule-compliant programs, both now and under any conceivable revision of the Rule, would still have to address the unique security considerations appropriate to "customer information" systems and databases within the context of the institution's overall information security environment.

16 CFR 314.4, Required Elements of a Rule-Compliant Information Security Program

314.4(a), Designation of a "Qualified Individual" to Oversee and Enforce the Security Program (Allow designation of a team, not just an individual, based on clearly documented lines of accountability)

The FTC states in the NPRM that it proposes to change this required element from one that currently allows covered entities to "designate an employee or employees to coordinate your information security program" to one that requires institutions to "[d]esignate a qualified individual responsible for overseeing and implementing… and enforcing your information security program…." Ostensibly this is to "ensure that a single individual is accountable for overseeing the entire information security program and to lessen the possibility that there will be gaps in responsibility between individuals."[10]

This mandate, however, fundamentally conflicts with the principle established in 16 CFR 314.3(a) that institutions should develop and maintain security programs "appropriate to your size and complexity, the nature and scope of your activities, and the sensitivity of any customer information at issue." At many small-to-medium-sized institutions, team approaches to managing multiple IT functions are very common and

[10] Federal Trade Commission, "Standards for Safeguarding Customer Information (Safeguards Rule), 16 CFR Part 314" (Notice of Proposed Rulemaking), *Federal Register*, Vol. 84, No. 65, April 4, 2019, p. 13165 (https://www.federalregister.gov/documents/2019/04/04/2019-04981/standards-for-safeguarding-customer-information#addresses).

appropriate to their size and complexity as well as the nature and scope of their activities. In such contexts, designating a single individual may not be optimal or practical, nor may it realistically achieve the FTC's aim of ensuring clear lines of accountability for the information security program.

Instead of mandating a one-size-fits-all model, the FTC should reinforce the expectation that a compliant program, however structured, clearly delineate lines of authority, responsibility, and accountability for all aspects of the security program. The Commission should also expand the scope of institutional executives that a covered entity might designate as the point or points of convergence for those reporting lines, again noting that an institution's size and complexity or the nature and scope of its activities (e.g., the degree to which it relies on outsourced services) may lead to effective and appropriate executive oversight, individually or collectively, from a chief information officer, a senior IT director, a chief financial officer, or other senior administrator. In this regard, we note that the Commission does not specify what constitutes a "qualified individual." We believe this is appropriate and aligns with our previous recommendation that the FTC explicitly state that such determinations are a matter of institutional discretion based on the ability to make a reasonable case for the decisions made.

We would also note that, despite the Commission's statements to the contrary in the NPRM, one may reasonably assume that the specific reference to the role of chief information security officer (CISO) in the revised Rule will create the expectation in practice that having a role with that title is necessary to comply with the Rule. And yet, the FTC provides no information or analysis establishing that this is necessary and appropriate for all or even most covered entities given their size and complexity or the nature and scope of their activities. Furthermore, the Commission provides no basis for establishing that this is practically *achievable*—within six months of a revised Rule's publication—given all publicly available evidence of a severe, long-term imbalance between supply and demand in the market for information security professionals, including specifically in higher education.

For example, the "Cybersecurity Supply/Demand Heat Map" developed and maintained with support from the National Initiative for Cybersecurity Education (NICE) of the National Institute of Standards and Technology (NIST) shows that the number of unfilled cybersecurity positions nationwide reached nearly 314,000 from September 2017–August 2018, while the total employed cybersecurity workforce in 2017 was estimated to be roughly 716,000.[11] Meanwhile, between FY16 and FY18, the percentage of U.S. colleges and universities with a CISO only increased from 27% to 30%, with the prevalence of the CISO role varying greatly by institutional type. Only 6% of community colleges had a CISO by FY18, while 64% of public doctoral institutions had one.[12]

The NPRM's emphasis on the CISO role combined with its lack of analytical support for that emphasis and the limited supply of cybersecurity professionals nationwide and in higher education implies that the Commission accepts the need for institutions to define what constitutes a qualified individual to oversee their security programs based on their needs and contexts. And if that is the case, then the Commission should also accept that institutions are best positioned to determine the overall roles, responsibilities, and accountability structures for their information security programs, with the clear compliance expectation that their programs will explicitly delineate those features and how they are enforced.

314.4(b), Required Risk Assessment (Refocus the requirement on a risk assessment framework approach)

[11] "Cybersecurity Supply/Demand Heat Map," CyberSeek: https://www.cyberseek.org/heatmap.html, as of June 27, 2019.
[12] EDUCAUSE Core Data Service dataset as of July 1, 2019: www.educause.edu/research-and-publications/research/core-data-service.

We propose that the Commission consider revising the first sentence of this section with the following underlined text: "Base your information security program on a risk assessment framework that enables effective identification of reasonably foreseeable…" We recommend these edits so the element reflects the reality that meeting the requirements it contains likely entails a range of different risk assessments based on the systems, data stores, and operations involved; it is the results of these context-specific assessments that collectively inform the range of safeguards an institution must pursue to effectively and appropriately structure its security program. We also recommend that the Commission provide examples of risk assessments or risk assessment frameworks tailored to the Safeguards Rule to serve as models for covered entities to use in determining how best to comply with this element and its requirements.

The risk assessment framework an institution adopts provides a common foundation for the needed assessments and ensures the consistency and alignment between them that allows for the institution's overall safeguards approach. Adjusting this element of the revised Rule to emphasize not a single risk assessment, but rather an overall risk assessment framework, may also help in resolving a lack of clarity that we perceive in some of the element's requirements. For example, in the absence of further context, "unauthorized alteration" or "unauthorized destruction" could apply to situations that aren't generally security-related, such as software bugs or other technical glitches. A framework would provide the needed context to ensure the terms are applied within the intended scope of the Rule, and that they are understood and applied consistently across the range of assessments an institution may need to conduct. Likewise, a framework approach would give content to requirements such as the criteria for risk assessment and mitigation/management under 314.4(b)(1) and the timing of future risk assessments under 314.4(b)(2).

314.4(c), Design and Implementation of Safeguards

314.4(c)(1), Information System Access Controls (Clarify requirement in relation to cloud services): The requirement as written seems to assume institutionally controlled and operated systems. With vendor-supplied cloud services, however, the management of authentication and access for service provider staff that fall under the Rule definition of "authorized user" may be relatively generic based on support category as defined in the services contract. We propose that the Commission make clear that the service provider oversight provisions of 314.4(f) are sufficient to address this issue.

314.4(c)(2), Inventory Organizational Resources Relevant to Business Purposes (Confine scope to systems and data related to "customer information"): Even set in the context of the risks that the institution identifies based on its risk assessment (framework), the scope of this requirement might easily be misinterpreted to extend well beyond those systems, data stores, and operations directly related to the privacy and security of "customer information." Therefore, as with our discussion of the proposed "information system" definition, we recommend that the Commission revise the requirement to clarify that its scope (and that of 314.4(c) generally) is limited to the systems, data stores, and operations directly related to the privacy and security of "customer information."

314.4(c)(3), Physical Location Access Restrictions (Confirm institutional discretion in determining relevant spaces): Given the open, decentralized nature of fundamentally academic institutions, we request that the Commission affirm in the Rule that compliance with this requirement is predicated on the institution providing a reasonable basis in its information security program for the physical locations identified for restricted access and the access restrictions implemented. This is particularly necessary given the breadth with which "containing customer information" could be interpreted in relation to our highly decentralized operating and service environments.

314.4(c)(4), Data Encryption (Provide examples of appropriate encryption methods, especially in relation to cloud services): The direct reference to "customer information" in the requirement is appreciated in that it reinforces the limitation on the relevant scope, which should help institutions avoid expensive acquisitions and implementations of encryption applications beyond those that are necessary to meet the requirement or otherwise serve the mission and operations of the institution. However, the Commission might consider supporting this requirement through resources that identify examples of encryption methods it considers appropriate to different aspects of handling or sharing "customer information"—for example, in providing consumers with online access to their own records. This would help covered entities to better understand the FTC's perspective on compliance in this area and address it in relation to their industry standards. Facilitating such understanding may be particularly important as institutions work with service providers to source relevant systems and data storage/access via cloud environments and provide appropriate oversight per 314.4(f) in the process.

314.4(c)(5), Secure Application Development Practices/Application Security Testing Procedures (Clarify institutional ability to demonstrate compliance via appropriate service contract provisions): The requirement clearly ties the applications it covers to "customer information," which is greatly appreciated. However, colleges and universities in general may find it financially and technically infeasible to independently test third-party applications on an ongoing basis, particularly without clarity on the extent of testing necessary to ensure compliance. This may particularly be the case in the context of cloud services, where institutions may not have, and generally cannot reasonably be expected to have, access to the service provider's code and technical infrastructure. We recommend that the Commission rewrite this requirement to clarify that provisions in purchase or service agreements requiring industry-standard testing and validation of supplied applications or services, in conjunction with the provider oversight requirements under 314.4(f), would be sufficient to establish compliance.

314.4(c)(6), Multi-Factor Authentication (MFA) (Maintain institutional discretion to apply MFA to systems and networks based on the institution's risk assessment): As institutions that are fundamentally academic and not financial services in nature, our network environments are not designed to operate along the same lines as a true financial institution, and it is not clear that they reasonably could or should be. Implementing MFA for any individual accessing customer information could be seen as extending to students and families themselves, which may not fit with the way such information is made available in conjunction with other forms of student data and records. Utilizing MFA for any individual accessing an internal institutional network assumes a segregated network architecture that is generally not applicable to our environments as compared to authentication and access at the application or database layer.

A broad survey of colleges and universities shows that approximately three-quarters of those responding are tracking MFA developments or planning to implement MFA to some extent, or have already partially deployed MFA; less than one-in-five, however, have deployed MFA institution-wide,[13] which this provision as written may require. At a minimum, this gives further weight to our recommendation for a substantially longer, more viable compliance timeframe than the six months currently proposed under 314.5.

More broadly, though, it illustrates the importance of the FTC revisiting how a specific, blanket requirement like this comports—or actually may not comport—with the long-standing principles of 314.3(a). The Commission is essentially mandating MFA regardless of the size and complexity of our institutions or the nature and scope of their activities, or how it does or doesn't fit with the underlying technical infrastructure that is based on those

[13] *The EDUCAUSE Information Security Almanac*, EDUCAUSE, April 2019, p. 2 (https://library.educause.edu/resources/2019/4/the-educause-information-security-almanac-2019).

parameters. In the absence of a clear delineation by the Commission of what alternatives an institutional information security executive might approve that the Commission considers reasonably equivalent, and assurance that they are reasonably applicable in our contexts, that pressure release valve in the requirement seems unlikely to release much pressure.

We recommend instead that the FTC adopt language that clearly allows an institution to establish compliance by illustrating in its security program the reasonable bases on which it has or hasn't applied MFA to relevant systems and networks, consistent with its size, complexity, nature, and scope. Again, the Commission should consider this proposal in light of the growing trend in higher education toward cloud services, where standard contracts and service provider capabilities may require time to evolve.

314.4(c)(7), Audit Trails (Revise to focus on system logs and account for cloud services, where access to logs or other relevant information may not be readily available): We recommend revising the text of this requirement to read, "As appropriate and feasible, incorporate the collection and review of system logs into the information security program to facilitate detection and response to security events." In the experience of higher education information security professionals, the term "system logs" is a more meaningful and consistently used term in the field than "audit trails." In addition, given the accelerating transition to cloud services, institutions may not have ready, direct access to system logs, nor would the relevant incident tracking activities occur at the institutional level. Service provider responsibilities to inform and support institutional incident response, of course, would be addressed in the context of the provider oversight requirements of 314.4(f) and the institution's incident response plan as discussed under 314.4(h).

314.4(c)(8), Secure Disposal of Customer Information (Allow for "other legitimate purposes" as well as other legal/regulatory requirements): We propose revising the text of this requirement as follows: "Develop, implement, and maintain procedures for the secure disposal of customer information in any format that is no longer necessary for business operations or other legitimate purposes, except where such information is otherwise governed by law or regulation, or where…" Even though the Commission explicitly does not define "legitimate business purposes," it is not clear that other legitimate purposes for which institutions might retain such data (e.g., institutional research, student analytics) could readily be classified as "business purposes" given how the "business" aspects of an otherwise academic institution are defined. Likewise, the "other legitimate purposes" that relevant data may serve are not always immediately apparent; the Rule should provide time and space for those purposes to evolve and not require an affirmative demonstration of current need to allow for retention as long as the security program establishes a reasonable basis for reassessment and subsequent disposal as appropriate. Finally, given that some states have laws governing the handling and disposal of relevant data, and those requirements may extend beyond the issue of data retention, allowing room in the requirement for the ways in which other relevant laws might govern institutional policies and procedures in this context would be helpful and appropriate.

314.4(c)(9), Change Management Procedures (Omit in favor of addressing this issue under our risk management framework proposal for 314.4(b)): The Commission asks whether this proposed requirement is more stringent than necessary or unnecessarily modifies the Rule without creating a material benefit to security. We would argue that the answer to both questions is "yes." Change management procedures are generally incorporated into an organization's IT operations for a variety of management purposes other than security, and the security considerations of a change in information systems and related aspects of the organizational IT infrastructure have to be considered and managed within that overall calculus. Given that, the provision as written is overly broad, and introducing it for the purposes stated in the NPRM may create expensive and unnecessary audit requirements to ensure compliance without producing benefits to the security of relevant data and systems.

Instead, we would recommend that the Commission discuss change management in the context of our previous suggestion about risk management frameworks under 314.4(b). Such frameworks generally address change management, but within the security concerns that the Rule is intended to address. Identifying the assessment of change management as a feature of an appropriate risk management framework would achieve the Commission's aims while maintaining the appropriate scope and focus.

314.4(c)(10) Monitoring of Authorized Users (Omit in favor of 314.4(c)(7) or revise to clearly tie the requirement's scope to "customer information and associated systems"): The Commission should consider whether the requirement identified under 314.4(c)(7) already addresses this consideration to an appropriate extent. It is also a fair question whether "use of" would cover "tampering with," such that the latter is redundant and might generate confusion about establishing compliance. In any case, academic institutions have a unique responsibility in terms of recognizing and respecting academic freedom and civil liberties, such that great care must be taken to ensure that the scope of any user monitoring under this proposed requirement strictly pertains to systems and data related to "customer information."

As currently written, the proposed requirement may be open to a much broader interpretation than intended, which again raises the specter of the Commission asserting compliance authority over the entirety of an institution's information security environment. For colleges and universities, that would take the Commission beyond the scope of GLBA. With that in mind, we propose that the Commission revise the requirement to ensure clarity of scope throughout: "Implement policies, procedures, and controls in relation to customer information and associated systems designed to monitor the activity of authorized users and detect unauthorized access or use of customer information by such users."

314.4(d), Monitoring and Testing Safeguards (Omit in favor of a proposed revision to 314.4(g) or revise to tie the requirement's scope clearly to "customer information" and relevant systems): The Commission should strike this requirement in favor of revising the proposed 314.4(g) to replace "the testing and monitoring required by paragraph (d) of this section" with "periodic assessment of the program." The expectation that a covered entity will periodically evaluate its information security program, including the key features and functions of the safeguards it employs, is certainly well-established and reasonable. However, the requirement as written is fundamentally in conflict with the long-standing core principles of 314.3(a) that place information security planning and development in the context of an institution's size and complexity, as well as the nature and scope of its activities. Whether continuous monitoring or annual penetration testing with biannual vulnerability assessments is or is not a reasonable expectation very much depends on those factors.

Combined with the overly broad definition of "information system" as previously discussed and the lack of a reference to "customer information" to provide appropriate scope, the proposed requirement appears to place the Commission in the position of asserting authority over information security planning and management for the entire institution. This seems to reflect an implicit assumption that extending the FTC's reach to such an extent is the only way to ensure the security of systems and data relevant to "customer information." Perhaps the Commission's view is appropriate for actual financial institutions. For fundamentally academic institutions, for which the relevant systems and data are but component parts of a much larger IT environment predicated on academic needs and functions, it constitutes the inappropriate overreach that the principles of 314.3(a) were implicitly adopted to avoid.

Continuous monitoring poses severe, expensive challenges for the highly decentralized systems, services, and data stores reflective of the academic mission that the overall IT environment of a college or university is designed to serve. The alternative—annual penetration testing with biannual vulnerability assessments—would constitute an equally or more expensive unfunded mandate unsupported by agency analysis establishing the

necessity and appropriateness of this approach for all colleges and universities regardless of their size and complexity or the nature and scope of their activities.

At a minimum, the Commission should edit the proposed 314.4(d)(1) and (2) to clearly limit the scope of the requirement to systems and data directly related to "customer information" as defined by the Rule pursuant to GLBA; it should also replace "Regularly test or otherwise monitor" with "Periodically assess" and strike (d)(2)(i) and (d)(2)(ii) to reaffirm the institution's discretion to determine what constitutes an appropriate, effective security program based on its size, complexity, nature, and scope:

> *(d)(1) Periodically assess the security of the customer information you hold, including the effectiveness of the information security program's key safeguards, with a specific focus on the controls, systems, and procedures designed to detect actual and attempted attacks on, or intrusions into, systems directly related to the management, processing, and/or storage of customer information.*
>
> *(d)(2) The periodic assessment of customer information security may include continuous monitoring or penetration testing and vulnerability assessments as appropriate to the size and complexity of the institution, the nature and scope of its activities, and the sensitivity of any customer information at issue.*

314.4(e), Human Resources Policies and Practices for Information Security Personnel (Omit to avoid inappropriate intrusion on matters best addressed by the institution based on its size, complexity, nature, and scope)

We applaud the Commission for specifically not defining what constitutes "qualified" or "key" information security personnel as those determinations are more appropriately made by the institution given its size, complexity, nature, and scope. Compliance in relation to these personnel considerations can and should be based on a reasonable case by the institution, as presented in its information security program, for what constitutes "qualified" and "key" given the institutional context. And as previously discussed, this institutional discretion is particularly important for small and mid-sized colleges and universities, especially those in rural areas, when contemporary data show a cybersecurity labor market that may have half as many unfilled cybersecurity positions as there are persons employed in the field.[14]

This proposed requirement as a whole, however, represents a broad new assertion of regulatory authority by the Commission to direct the personnel practices of institutions without a full consideration of the implications of that assertion. The concepts presented in the proposed requirement could be considered effective practices that the FTC might join with relevant professional and industry groups to promote, and we would encourage the Commission to take this path. As a compliance matter, though, neither the proposed Rule text nor the NPRM provide a solid basis for determining how the Commission would hold covered entities accountable for this requirement. While this likely stems from the Commission's commendable desire to maintain institutional flexibility and discretion based on context, covered entities will likely have significant concerns about how they can reasonably conclude whether they are or are not in compliance.

Any effort to be more specific, however, would lead the FTC down the road to setting human resources standards and policies for all covered entities in relation to their information security functions. And yet, for example, the FTC rightly states the following in the NPRM: "The proposed amendment does not define 'key

[14] "Cybersecurity Supply/Demand Heat Map," CyberSeek: https://www.cyberseek.org/heatmap.html, as of June 27, 2019.

personnel' as the Commission believes that which personnel are 'key' will vary considerably from entity to entity and that each financial institution will need to determine which employees must maintain this knowledge based on their structure and risk assessments."[15] From this, one may infer that the Commission recognizes the centrality of institutional discretion in setting personnel policies and practices in relation to a given context. That in turn begs the question of what the Commission seeks to achieve by creating compliance expectations that ultimately resolve to the current Rule's starting point—institutional determinations of what is or is not necessary and appropriate given the institution's size, complexity, nature, and scope. Thus, it becomes an open question whether a proposed Rule requirement is the most effective and appropriate way to accomplish the Commission's objectives, as compared to the outreach and engagement we recommended in our prior comments.

314.4(g), Assessing and Updating the Information Security Program (See our previous points related to 314.4(d) on pages 14-15 of these comments)

314.4(h), Establish a Written Incident Response Plan (Rephrase to emphasize timely response to security events affecting data under the institution's control and recovery "as quickly and effectively as feasible")

We would argue that the text of the requirement as currently written is too expansive. Given the range of security events that might occur and their potential impacts on institutional capacity to recover, establishing an incident response plan that will allow an institution to "respond to, and recover from, *any* security event materially affecting… customer information" (emphasis added) may simply not be feasible. In addition, "in your possession" does not adequately account for the use of cloud services, where the institution would not directly possess the relevant data but would maintain responsibility for ensuring it is safeguarded per other provisions of the Rule. *Therefore, we would recommend that the Commission write the requirement as follows: "Establish a written incident response plan designed to respond in a timely fashion to a security event impacting the customer information for which you are responsible and to recover from it as quickly and effectively as feasible."*

Regarding the Commission's specific questions about this proposal as stated in the NPRM, we would not recommend adding reporting to the FTC as a requirement of the institution's incident response plan. In the absence of greater clarity about the role the FTC would play in supporting institutional response to a "security event" as defined by the Rule, introducing an FTC reporting requirement would simply add another layer on top of an already crowded list of federal and state law enforcement contacts and state breach reporting requirements that colleges and universities must currently manage during a relevant event. If the FTC continues to consider this option, despite the additional administrative burden it would create and the uncertain benefits that might result from it, the Commission should certainly consider our previous points on the definition of "security event" in relation to this proposed requirement. For example, the unauthorized acquisition of encrypted data when the encryption key has not itself been compromised does not lead to the unauthorized access or misuse of such data, and thus should not constitute a reportable event, consistent with the "substantial harm or inconvenience" standard established under the current 314.3(b)(3). Moreover, with that standard in mind, any reporting requirement should clearly and directly relate to "security events" and not any general incidents an institution may encounter.

[15] Federal Trade Commission, "Standards for Safeguarding Customer Information (Safeguards Rule), 16 CFR Part 314" (Notice of Proposed Rulemaking), *Federal Register*, Vol. 84, No. 65, April 4, 2019, p. 13169 (https://www.federalregister.gov/documents/2019/04/04/2019-04981/standards-for-safeguarding-customer-information#addresses).

Likewise, making any such reports public could lead to additional efforts by malign actors to compromise the security of the given institution's customer information, and thus should not occur or should only occur after the event has been resolved and the institution has had the opportunity to sufficiently address any underlying security concerns. Along the same lines, any reporting requirement should allow for notification delays based on law enforcement requests related to ongoing investigations, as law enforcement efforts to apprehend malign actors benefit the security of institutions and individual consumers in general.

314.4(i), Annual Board Reporting (Require instead that security programs clearly explain the basis and rationale for how senior leadership and governance bodies are regularly informed and engaged)

The Commission's proposed annual reporting requirement to the institution's governing board regarding Safeguards Rule compliance would have the effect of shifting the emphasis of information security within the institution from a risk management focus to a compliance focus. Of course, the Rule stresses the development and maintenance of the institutional information security program based on an assessment of risk; the proposed requirement as written, however, directs the focus of information sharing about the program with the institutional governance process toward reviewing and delineating the Rule's respective requirements and the institution's steps to meet them. It also creates the expectation that a single, overriding report is the best way to effectively engage institutional governance in information security oversight when and where that is appropriate. Finally, the provisions of the proposed requirement under (i)(2) call for reporting a level of detail that may not serve board oversight well, as the expansive list of specific information involved may lead the governance body to "miss the forest for the trees" and not direct the board's attention to providing the strategic guidance that is its core function.

In the alternative, we propose that the Commission recast the proposed requirement to focus on regular reporting about the institution's information security program to the institution's senior leadership and governance body per the process and schedule established in the program. This would include delineating a reasonable basis for the reporting needs, process, and schedule set forth in the program as informed by the elements and requirements of the Rule. This approach would meet the Commission's implicit emphasis on ensuring an overt, sustained engagement of the institutional governance process in matters pertaining to appropriately securing customer information while again basing the terms of that engagement on the institution's assessment of its needs given its size, complexity, nature, and scope.

On the Commission's specific question about possibly requiring Board certification of compliance with the Rule, we would recommend that the Commission not impose such a mandate. As a practical matter, governing boards generally will not have the knowledge and expertise to independently certify the institution's compliance with the Rule. That alone makes the proposed requirement inherently and excessively burdensome, since compliance could not be achieved in most cases without employing external, specialized auditors. Securing audit services of that type would require significant institutional expense, which the annual reporting requirement would make a major, new, yearly expense. The Commission provides no analysis establishing that such an expense would likely generate equivalent benefits to the safeguarding of "customer information" and associated systems, or that this is the best, most appropriate path for all covered entities of all types to ensure effective governance oversight of their information security programs.

Given the diversity of institutional size, complexity, nature, and scope, we would urge the Commission instead to recast this requirement in terms of the institution explicitly identifying within its security program the reporting process it utilizes to ensure appropriate governance oversight of the program. This explanation should include the basis on which it has structured the reporting process, addressing matters such as timeframe, content, and incorporation of input or explicit direction into the program. In this fashion, the Commission can achieve its aim

of ensuring an effective level of engagement by the institutional governance body in matters pertaining to the security of "customer information" without imposing a compliance requirement that may present an inappropriate, unaffordable burden.

Conclusion

We again thank the Commission for the opportunity to provide input on its proposed revisions to the Safeguards Rule. As we have illustrated throughout our comments, the distinction between colleges and universities as academic institutions and their technical status as "financial institutions" under the Safeguards Rule has major implications for the FTC's proposals. By possibly moving beyond the broad but limited provisions of the current Rule, the Commission threatens to undermine the flexibility and discretion inherent in the Rule that allows it to bridge this distinction and work in the *higher education* context.

We continue to urge the Commission to focus on engagement and guidance to expand awareness and adoption of effective practices related to the security of "customer information." That is more likely to achieve the Commission's goals than the introduction of a range of new provisions that in many cases are subject to interpretation in ways that could easily frustrate compliance. If the Commission continues with its existing proposals, we hope we have made clear the need for a revised Rule to explicitly state that (i) institutions retain the discretion to define essential aspects of the various elements and requirements based on their context per 314.3(a), and (ii) the scope of the Rule's provisions is limited to data and systems directly related to the security of "customer information." We also hope that we have highlighted the importance of revisiting a number of proposed changes to ensure they can appropriately accommodate the growing prevalence of cloud services.

Most importantly, we believe we have established the necessity of revising the compliance timeframe identified in 314.5. The range and complexity of the changes the Commission proposes render a six-month deadline simply infeasible for many if not most colleges and universities. A two-year horizon with a one-year deadline for producing an implementation plan allows for a viable approach to compliance that the Commission should consider. Also, we specifically ask that the FTC revise 314.6 to ensure that small colleges and universities can rightfully claim the exceptions that the provision identifies.

The revisions that we suggest for other proposed requirements would improve their appropriateness and effectiveness. We encourage the Commission to adopt them in the final Rule to support our shared goal of continuous improvement in information security. If further discussion of our comments would better inform FTC deliberations, the higher education community stands ready for that dialogue.

Sincerely,

Ted Mitchell
President

On behalf of:

American Association of Community Colleges
American Association of State Colleges and Universities

American Council on Education
American Dental Education Association
Association of American Universities
Association of Public and Land-grant Universities
Council for Christian Colleges & Universities
EDUCAUSE
National Association of College and University Business Officers
National Association of Independent Colleges and Universities