February 7, 2021

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 Supplemental Notice of Proposed Rulemaking, "Standards for Safeguarding Customer Information" (Safeguards Rule, 16 CFR 314, Project No. P145407), December 9, 2021—Proposed Security Event Reporting Requirement

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 supplemental notice of proposed rulemaking (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 December 9, 2021, at:

https://www.federalregister.gov/d/2021-25064

We thank the Commission for the opportunity to provide input on its proposal to add a further requirement to its Safeguards Rule, namely that covered entities—including colleges and universities—would have to report to the FTC any "security event" in which:

- The entity has determined that the misuse of customer information has or is reasonably likely to have occurred, and
- At least 1,000 consumers have been or reasonably may have been affected.

The Commission's stated rationale for proposing the new requirement is that reporting of this type "would ensure the Commission is aware of security events that could suggest a financial institution's security program does not comply with the Rule's requirements, thus facilitating Commission enforcement of the Rule." However, the Commission identifies a further rationale in its analysis of the proposed rule in relation to the Regulatory Flexibility Act, where it states: "To the extent the reported information is made public, the information will also assist consumers by providing information as to the security of their personal information in the hands of various financial institutions."

The Commission asks respondents to consider several questions in commenting on the potential security event reporting provision it presents, and we believe that effectively answering them requires placing one's responses in the context of the Commission's stated

reasons for proposing the new requirement. In other words, will the options implied by the Commission's questions actually serve or detract from its identified objectives? It is through that lens that we offer our following comments.

Topic 1—Information to Report: Is the proposed list of elements that covered entities would have to report to the FTC under the new provision sufficient? Should more or less information be required?

For security events of the type identified above, the Commission would require covered entities to report:

- The organization's name and contact information,
- A description of the types of information involved,
- The date or date range of the event (if that information is available), and
- A general description of the event.

The Commission proposes to require reporting of this general information only in relation to a particular subset of security events—those that affect 1,000 or more consumers and for which the covered entity has determined that misuse of customer information has happened or is reasonably likely to happen—to limit the potential reporting burden on covered entities. We appreciate the Commission's sensitivity on the issue of reporting burden since many colleges and universities already face an extensive array of cybersecurity reporting requirements under existing laws and regulations. We agree that the proposed reporting elements should enable covered entities to provide the Commission with the information it needs to consider potential Safeguards Rule compliance issues while mitigating the burden they face in doing so, and we thank the Commission for seeking to strike this careful, necessary balance.

Topic 2—Reporting Threshold: Is the FTC's proposed threshold for security event reporting sufficient? Should covered entities be required to report events in which the misuse of customer information is only possible—not determined or reasonably likely? Should the new requirement include a carve-out for events involving encrypted data?

In 16 CFR 314.3(b), the Safeguards Rule identifies protecting customers from "substantial harm or inconvenience" as one of its primary objectives. The Commission's proposed new requirement sets a threshold for security event reporting that is consistent with this objective as well as the compliance interests that the Commission has identified as the core rationale for its proposal. Security events in which the covered entity has determined that the misuse of customer information has occurred or is reasonably likely to occur would generally raise the "substantial harm or inconvenience" concerns that the Rule is intended to address, and reports on events of this type involving 1,000 or more consumers, with the information reported following the elements identified in the FTC's rulemaking notice, would provide the Commission with a reasonable basis for considering whether there are compliance issues it may wish to explore further.

Expanding the universe of required reporting into the realm of the possible, however, risks introducing a high degree of uncertainty into the reporting process that would likely lead to burdensome over-reporting with negative effects for the FTC as well as covered entities.

Taking the Commission's encryption question as a starting point for this discussion, cybersecurity practice generally assumes that encrypted data remains secure so long as encryption that meets or exceeds industry standards has been utilized and there is no indication that the encryption involved has been compromised. This is consistent with the risk management focus on which effective cybersecurity practice is based, as reflected in the Rule itself—this principle almost certainly underpins the requirement for encrypting customer information at rest and in transit over external networks that the Commission introduced as part of its recent Safeguards Rule revisions. However, no encryption method is completely foolproof. It is still possible that high-quality, industry-standard encryption may be compromised—the risk of that occurring is just exceedingly small and thus considered acceptable in all contexts relevant to the Safeguards Rule.

Essentially, moving from "reasonably likely" to "possible" would alter the risk calculation of security event reporting in a fashion that eliminates the careful balance the Commission initially intended to strike. Covered entities would likely report exponentially more cases out of an abundance of caution, with the additional time, effort, and expense that entails, given that the threshold for possible misuse of customer information is so much lower (even when the risk is negligible for all practical purposes). This, in turn, would substantially degrade the value of security event reporting to the Commission's efforts at compliance evaluation since the overall volume of reports would make it significantly more difficult to identify cases of legitimate concern. Of course, the Commission could attempt to mitigate this effect by changing the standard to "reasonably possible," for example, but the risk calculus on reporting-versus-not-reporting would remain fundamentally altered to the detriment of covered entities and the FTC's compliance objectives. The degree of uncertainty around what may be possible is just altogether greater than it is around what may be likely.

Returning to the question of whether to automatically exclude events involving encrypted data from the reporting requirement, as we noted above and similarly argued in our comments on the recently adopted revisions to the Safeguards Rule, the probability of encrypted data being subject to misuse is extremely low in the absence of the encryption method having been compromised. Thus, covered entities would generally determine that they do not have a reportable event when encrypted data is involved and there is no reasonable basis for thinking that the encryption has been or likely could be compromised. Given this reality, it would support the Commission's goal of minimizing the reporting burden on covered entities as well as the encryption mandate that the Safeguards Rule now includes to state explicitly in the proposed requirement that covered entities do not have to report events involving encrypted data when there is no credible basis for determining that the encryption has been or is reasonably likely to be compromised.

Topic 3—Reporting Deadline: Is the thirty-day deadline for reporting a covered event to the FTC appropriate, or would a shorter period be viable?

Given the range of issues that a covered entity may have to manage with any particular security event and the complexity it might encounter in determining whether an event meets the reporting criteria, we would argue that a thirty-day reporting deadline strikes an appropriate balance. Based on the elements that an entity would be required to report, the proposed reporting timeframe should provide an entity with adequate time for initial incident assessment and response while addressing the Commission's interest in compliance

evaluation.

We would not agree that a shorter reporting period is appropriate. The Commission has stated that it wishes to mitigate the potential burden of its proposed reporting requirement to the extent it can while advancing the goal of Safeguards Rule compliance. In the context of a security event, though, incident assessment and response, which includes addressing the security of customer information and, when necessary, restoring normal operations, should take precedence. A shorter reporting period would risk infringing on effective execution of an entity's response efforts, particularly in more complex cases, without contributing substantially to the Commission's consideration of compliance issues.

The Commission has proposed a set of reporting elements designed to make the reporting burden on covered entities manageable while ensuring its ability to evaluate cases of potential concern. That balance could easily be lost, however, if a tighter deadline forces entities to address compliance ahead of security. With that in mind, we propose a modest edit to the draft text of 314.4(j) in addition to expressing our support for the Commission's thirty-day reporting deadline. We ask the Commission to consider substituting "without unreasonable delay" for "as soon as possible": "…, you must notify the Federal Trade Commission as soon as possible without unreasonable delay, and no later than…" Again, since the factors involved in any given security event may be more or less demanding on an entity's time, effort, and resources, we suggest that the timeliness of response prior to the thirty-day deadline should be framed in terms of the conditions an entity is working to overcome.

Topic 4—Law Enforcement Requests: Should the proposed Safeguards Rule reporting requirement allow for a prevention of or delay in reporting based on a law enforcement agency's request? Would such a block or delay only be necessary to the extent that reports are made publicly available?

As we proposed to the Commission in our comments on the revised version of the Safeguards Rule, we believe that a covered entity should be allowed to honor a law enforcement agency request to delay reporting about a security event to the FTC in support of the law enforcement investigation of that event: "…, 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."

The Commission's valid interest in information to support its regulatory oversight responsibilities can still ultimately be served without requiring a covered entity to take a step in a given case that a law enforcement agency has identified as contrary to its efforts to hold accountable those who are criminally responsible. Given the information that an entity would have to report under the FTC's proposed provision, we believe that such law enforcement requests would be rare and of limited duration in any case. However, since they would generally be related to investigations of criminal conduct or may entail other national interests, we would argue that covered entities should be able to comply with law enforcement requests to delay Safeguards Rule reporting as long as the law enforcement agency deems it necessary for the investigation in question.

Furthermore, we believe that the ability to honor law enforcement agency requests should not be predicated on whether the FTC would or would not make covered entity reports public. If a law enforcement agency asks an entity not to share any information about a case outside the bounds of its investigation, that should be the determining factor given the considerations identified above. The Commission and the law enforcement agency or agencies involved could certainly work to reach an accommodation that the entity could then honor, however, in the unlikely event that a significant delay and particularly significant compliance concerns on the part of the Commission were involved. With this in mind, we propose that the FTC consider including in its reporting process a mechanism that would allow an entity to inform the Commission about the need to delay reporting at the request of law enforcement. This would allow for a dialogue about the request between the entity, the FTC, and the relevant law enforcement agency/agencies.

Topic 5—Public Availability of Reports: Should security event information reported to the FTC be released publicly? Should covered entities be able to request that a report or reports be kept confidential? Should they be able to request a delay in the public release of a report or reports? If so, on what basis should they be able to request that reported information be kept confidential or only released after a certain period?

We note that the supplemental notice for the current regulatory process already assumes that the FTC would make the reports required by the Rule publicly available via an online database. And as we discuss toward the end of the first page of these comments, the Commission believes that making such information public would help consumers by giving them a sense for how securely covered entities are managing the consumers' personal information.

The information that the proposed reporting provision would require covered entities to submit, however, is appropriately calibrated to help inform the Commission's compliance efforts without creating an undue reporting burden. The required reporting elements would not give a consumer of any particular entity, or even necessarily a group of such consumers, insight into the security of his/her/their personal information. While the elements would serve to give the Commission as a regulator an effective basis from which to consider whether a given case or cases bears more focused attention, they would only allow for a very general overview of an event from a consumer standpoint.

In the meantime, having even a general report to the FTC about a security event made public could serve to encourage additional attempts to compromise an entity's cybersecurity. Such information may be more than sufficient to encourage other malign actors to attempt to find and exploit the issue that led to the initial event, thus placing a premium on the covered entity in question having an appropriate amount of time to fully address incident response and remediation before a report might be made publicly available on something like a single, national website that covers all events of a certain type across all covered entities under the Commission's purview.

It is also worth noting that provisions of state law or regulation may affect the capacity of colleges and universities in a given state to report security event information. For example, state law in Florida makes significant categories of cyber incident information held by state

agencies—which includes public colleges and universities—confidential and exempt from public disclosure in cases where the public availability of such information might facilitate further compromise of an agency's cybersecurity. The law does allow that otherwise "confidential and exempt" information "may be made available to… a federal agency for cybersecurity purposes," but the potential for confusion and friction between the institution, the state, and the Commission about where the respective state and federal requirements may or may not align could still be considerable.

Given these factors, we recommend that the Commission take additional time to engage with covered entities and research the potential for legal and regulatory conflicts in relation to publicly releasing covered entity reports before deciding whether to proceed with making such reports publicly available and under what conditions. Significant unintended consequences could flow from such a decision with adverse impacts for consumers, customers, and covered entities alike. In the absence of agreement that this proposed step requires further study, though, the FTC should revise the proposed rule to include a one-year delay in the public release of required reports from the date of their initial submission. The Commission's reporting process should also include a mechanism through which a covered entity may request that the FTC maintain the confidentiality of a report or reports based on cybersecurity, operational, and/or other legal and regulatory compliance considerations.

Covered entities that encounter security events that might require reporting under the proposed provision will vary widely in terms of the organizational resources they bring to the challenges such events raise. The nature of relevant security events themselves will also vary considerably from case to case. Any public release of information about an event, however general the information may be, must not negatively affect the ability of the entity to respond effectively. This requires taking into account that the resource challenges and organizational capabilities of an entity may combine with the complexity and cost of a given event such that the entity may require significant time to fully remediate the system or systems in question. Likewise, a public release of information before the institution has had the opportunity to fully inform the consumers and other stakeholders most directly affected by an event risks creating a counterproductive atmosphere of anxiety and concern across an entity's consumers and stakeholders in general. State breach notification requirements may lead to some measure of public notice prior to what would be considered ideal for incident response. However, the collection and public release of such information at a national level from a single, online source would introduce a new level of risk in terms of cybersecurity.

A one-year delay in publicly releasing covered entity reports would ensure that organizations have sufficient time to resolve the challenges a reportable security event has raised, enhance cybersecurity protections where necessary, and reach as many of those directly affected as possible. In addition, it would allow for this important set of objectives to be accomplished without negatively impacting the Commission's stated objectives for the proposed reporting requirement. The Commission would have access to the information for its compliance evaluation purposes, and the general public would have access to an ongoing record of compliance information that would allow it to understand the compliance picture concerning a covered entity as well as covered entities in general over time. Moreover, as we have illustrated, other legal and regulatory requirements regarding cyber incident reporting and breach notification may present covered entities, the Commission, and other oversight bodies with a tangled set of considerations to navigate. Ensuring that the proposed reporting

process provides adequate time and opportunity for those to be raised and resolved before reports are made public by the federal government would only serve to support cybersecurity at the multiple levels of society and government at which it must be addressed. With these issues in mind, we encourage the Commission to adopt our recommendation for a one-year delay in publicly releasing reports submitted under the proposed Safeguards Rule provision.

Topic 6—Existing Reporting Requirements: In lieu of establishing a Rule-specific reporting requirement, should the Commission instead only mandate that a covered entity notify it of a security event when the entity must provide notice to another government agency under a different law or regulation? How would this affect the Commission's oversight of Safeguards Rule compliance, the burden that covered entities face, and the consistency of the information that the Commission receives?

As stated in the Commission's rulemaking notice, the information it seeks to have reported is intended, first and foremost, to inform its oversight of Safeguards Rule compliance. While required reports to other governmental agencies and oversight bodies may include information that the Commission would find relevant to its purposes, trying to use those reports to meet the Commission's objectives would most likely require a broader array of otherwise unnecessary engagements with a wider range of covered entities as FTC staff seek to resolve questions or knowledge gaps arising from information assembled and organized in relation to other legal and regulatory provisions. Additional problems could arise from this approach if the laws and regulations under which the reports were originally produced allow for the confidentiality of the reports to be maintained while the FTC's process, as currently envisioned, would lead to their public release.

To the extent that some of the information included in a report to another governmental entity based on its requirements might be relevant to Safeguards Rule reporting, covered entity staff would probably be best positioned to extract and share relevant points with the FTC based on the required reporting elements identified in the current rulemaking notice. Therefore, as long as the balanced approach described in the notice is maintained, it would likely minimize the reporting burden for covered events to a greater extent than sharing other types of potentially relevant reports with the Commission, given the additional process and communications overhead that trying to fit those reports into the Commission's needs may generate. With this in mind, we support implementing the Commission's reporting provision as proposed in the current rulemaking notice.

Topic 7—Need for Reporting Requirement: Should the Safeguards Rule include a reporting provision?

The Commission introduced the concept of Safeguards Rule reporting in the notice of proposed rulemaking concerning the broad set of changes to the Rule that the FTC recently adopted. It did not at the time, however, provide information about the nature and scope of the reporting it was considering. As a result, we commented then that such reporting seemed unnecessary given the many existing cyber incident reporting and/or notification requirements that colleges and universities already must address. The additional context provided by the current notice clarifies the parameters for reporting under the Rule, though, and reflects a commitment on the part of the Commission to minimize the reporting burden

on covered entities while seeking general information to inform its regulatory oversight. With this in mind, we do not object to a reporting requirement of the nature and scope currently proposed, with the caveat that reports submitted under the Rule should not be made public for one year to allow sufficient time for covered entities to fully address incident response, consumer/stakeholder communications efforts, and/or other relevant legal and regulatory concerns.

Topic 8—Consumer Notification: Should a consumer notification requirement be added to the Safeguards Rule in addition to the proposed requirement for security event reporting to the FTC?

As noted previously, colleges and universities already must manage a wide range of notification requirements. Events of the type that the Commission has identified for reporting to it under the Safeguards Rule would generally trigger notification to affected students, faculty, staff, and/or other stakeholders under the laws and/or regulations of multiple states, and multiple state requirements can easily come into play for colleges and universities given the many states from which our institutional communities may draw. Therefore, we recommend that the Commission work with covered entities to better understand the nature and scope of the notifications that entities must already provide before considering whether to add another requirement to the Safeguards Rule. Information of this type would allow the FTC to evaluate whether existing breach notification regimes already effectively address the situations it has identified in the current notice on Safeguards Rule reporting, which presumably would form the basis for a consumer notification requirement that the Commission might consider. Likewise, it would help the Commission and covered entities think about the potential for consumer confusion if a Rule-specific notification requirement was layered on top of other relevant notification processes.

Conclusion

We appreciate the Commission's willingness to consider how best to balance its information needs with the burden that meeting those needs might impose on covered entities. We believe that the Commission has achieved a reasonable balance with the reporting provision proposed in its supplemental notice, and thus it should proceed with the provision as written for the most part. As we have established, though, the interests of the Commission, covered entities, consumers, and the public in general would be best served by delaying the public release of any reports submitted under the proposed requirement by one year to allow for effective incident response, communications with affected consumers as well as organizational stakeholders, and resolution of potential complications presented by other legal and regulatory requirements.

The Commission should also modify its proposed provision to ensure that covered entities can honor the requests of law enforcement agencies to delay reporting under the Safeguards Rule as necessary to support law enforcement investigations. In addition, we encourage the Commission to revise the text of the reporting requirement slightly to reflect that entities should submit required reports "without unreasonable delay, and no later than 30 days after the discovery of the event," recognizing that the timing of reporting within the given timeframe should be driven by the conditions a covered entity faces in addressing the security event in question.

Finally, since a covered entity would not consider an event involving encrypted data to be reportable in the absence of a valid concern about the integrity of the data's encryption, the Commission should state clearly in the reporting provision that events involving encrypted information are exempt from reporting unless a credible basis exists for determining that the encryption has been or might reasonably be compromised.

We thank the Commission again for this opportunity to comment on its supplemental notice regarding potential security event reporting under the Safeguards Rule. If we can assist the Commission further in its work by clarifying any of the points or recommendations we have made, we would be pleased to do so at the Commission's earliest convenience.

Sincerely,

Ted Mitchell
President

On behalf of:

American Association of Collegiate Registrars and Admissions Officers
American Association of Community Colleges
American Association of State Colleges and Universities
American Council on Education
Association of American Universities
Association of Catholic Colleges and Universities
Association of Governing Boards of Universities and Colleges
Association of Public and Land-grant Universities
Association of Research Libraries
Council for Christian Colleges & Universities
Council of Independent Colleges
EDUCAUSE
National Association of Independent Colleges and Universities