January 30, 2018

A. Wayne Johnson, PhD
Chief Operating Officer
Federal Student Aid
U.S. Department of Education
830 First Street, NE
Washington, DC 20002-5403

Dear Dr. Johnson:

I write to you on behalf of the colleges, universities, and organizations that comprise EDUCAUSE to highlight the strong interest we share with Federal Student Aid (FSA) in the security and integrity of federal student financial aid data. Given that shared interest, we hope FSA will work with our community to more effectively define FSA’s data breach notification and information security program reporting requirements. The office’s existing approach to compliance has generated significant concern that FSA is inadvertently detracting from the security efforts it seeks to bolster. We believe, however, that the security of institutionally held FSA data can be greatly advanced through a collaborative process involving FSA officials and higher education information security leaders. The goal of this effort would be to clarify FSA information security compliance guidance and processes, particularly as they relate to data breach notification, and revise them where necessary to support our shared data security objectives.

EDUCAUSE (www.educause.edu) is a nonprofit association and the foremost community of information technology (IT) leaders and professionals committed to advancing higher education. Our membership encompasses over 1,800 colleges and universities, over 400 corporations, and dozens of other associations, system offices, and not-for-profit organizations. EDUCAUSE strives to support IT professionals and the further advancement of information technology in higher education through analysis, advocacy, community-building, professional development, and knowledge creation.

For over 17 years, EDUCAUSE has supported the evolution of information security in higher education through the Higher Education Information Security Council (HEISC). ¹ HEISC members—including chief information officers (CIOs), chief information security officers

---

(CISOs), chief privacy officers (CPOs), and related professionals—collaboratively develop events, resources, and professional networks to bring about continuous improvement in the field.

For example, HEISC has maintained the *Information Security Guide: Effective Practices and Solutions for Higher Education*\(^2\) for over 15 years. It serves as a free resource on establishing and advancing an institution-wide approach to information security within the unique higher education context. Likewise, HEISC organizes the Security Professionals Conference,\(^3\) which convenes hundreds of higher education information security leaders and professionals each year to learn and grow together as a community.

Given our commitment to higher education information security, EDUCAUSE appreciates FSA’s interest in the field. We initiated direct dialogue with FSA on shared concerns, such as potential uniform federal guidelines for controlled unclassified information (CUI), in the fall of 2016. At that time, member CIOs and CISOs met with FSA Deputy Chief Operating Officer Matthew Sessa, FSA Chief Information Officer Keith Wilson, and their colleagues to discuss how FSA would collaborate with our members on implementing such guidelines. Since then, we have been pleased to work with Tiina Rodrigue, FSA senior advisor for cybersecurity, to inform development of the pending Gramm-Leach-Bliley Act (GLBA) Safeguards Rule\(^4\) federal single audit objective,\(^5\) as well as to have her speak at our 2017 annual conference.

These interactions give EDUCAUSE hope that FSA will work with our community to review and revise its information security compliance guidance and processes, specifically in relation to breach notification. Recent FSA compliance actions have raised significant concerns among our members about the scope of authority FSA is asserting, the basis on which it is doing so, and the lack of official documentation and processes for the asserted requirements.

**Recent FSA Compliance Activities**

In late 2017, FSA sent letters to various colleges and universities informing them that they were required to report alleged data breaches to FSA. These letters were addressed and delivered to the institutions’ presidents without prior outreach to the institutions’ designated points of

---


contact for FSA data. Institutions received one of two types of letters. One type stated that a breach or suspected breach of some kind, not necessarily of FSA data, had occurred at the institution, requiring it to now make a full accounting of its information security program. The other type of letter covered the same ground but added that the institution had failed to self-report the alleged breach or suspected breach, further increasing its potential compliance problems. The letters gave institutions thirty (30) days to formally respond to the allegations and referred them to resources for more compliance information, including:

- the 2016–2017 version of the *Federal Student Aid Handbook (Handbook)*;\(^6\)
- a July 2015 Dear Colleague Letter focusing on Gramm-Leach-Bliley Act (GLBA) Safeguards Rule compliance;\(^7\) and
- a July 2016 Dear Colleague Letter noting plans to implement a Safeguards Rule audit objective and highlighting other security references.\(^8\)

The letters cited volume 2, chapter 7, of the 2016–2017 *Handbook* (p. 2-155) as the reference for institutions’ responsibility to report “any known or suspected breaches” to FSA, although the text at that location does not address “suspected breaches” or point to other references.

In many instances, FSA sent these letters based on claims of possible breaches cited by online media, as indicated at the start of the letters themselves. To the best of our knowledge, FSA did not confirm with the institutions prior to the issuance of these letters whether the media reports provided an actual basis for concern about a breach or suspected breach, or that the alleged breach or suspected breach was related to FSA data. In essence, FSA asserted that an unconfirmed media report provided sufficient cause for it to assume that the institution had or should have suspected a breach, which should have resulted in a self-report to FSA, including a comprehensive, detailed review of the institution’s information security posture. Moreover, the letters generally did not provide sufficient information about the alleged breach or suspected breach to facilitate institutional identification and assessment of the purported incident. As a result, institutions often had to expend considerable time and resources just to determine the issue to which the letters might reasonably refer.

In addition to these letters, FSA officials made several public statements in the last half of 2017 that generated further concern about breach notification requirements and processes. It was


said on various occasions that notifications could be made via text message to an FSA official’s cell phone number; that blocked phishing attempts (a routine information security occurrence) constitute a suspected data breach that must be immediately reported; that “immediate notification” of a breach or suspected breach means that the institution must report on the “day of detection,” which does not afford an institution with the opportunity to conduct any analysis to confirm a possible incident or contact law enforcement; and that institutions must provide forensic images of allegedly compromised machines in making a notification. These statements have potentially controversial implications for issues such as due diligence, the appropriate use of institutional resources, and routine information security practices (e.g., incident investigation and confirmation). In addition, they raise concerns about the degree to which FSA has or hasn’t established a standardized, secure process for the receipt and storage of sensitive institutional information that also addresses key policy issues (e.g., the potential for Freedom of Information Act requests, the sharing of information with unaffiliated third parties).

Institutional Questions

These letters and statements raise key questions with which institutions are grappling:

1. What legal, regulatory, or contractual provisions define an institution’s information security and breach notification requirements with respect to FSA data?
2. What authority do those provisions give FSA to require that institutions notify it about all institutional data breaches or suspected breaches, even those not involving FSA data?
3. What authority do those provisions give FSA to require that institutions notify it about all suspected breaches of FSA data?
4. What is the definition of a “breach” or a “suspected breach,” and how is the notification process (including the legal, regulatory, or contractual provision defining “immediate” as “day of detection” in relation to unconfirmed incidents) publicly documented?

FSA Basis of Authority

FSA authority related to institutional information security practices, including breach notification requirements, appears to rest on (a) the GLBA Safeguards Rule compliance provision in the FSA Program Participation Agreement (PPA), and (b) the breach notification provision of the FSA Student Aid Information Gateway (SAIG) agreement. It is important to note, though, that various versions of these agreements are in force and that individual institutional agreements may not all contain the same contractual language, according to information we received from FSA. This calls into question the extent to which these
documents can form the basis of the “standard breach notification requirements” that are currently being communicated to institutions.

Assuming we have a correct understanding, we would urge FSA to document publicly the exact agreement text on which it is currently basing its guidance and how that compares to prior iterations of relevant text in versions of the PPA and the SAIG agreement that are still in effect. This will allow institutions to more easily assess their compliance obligations given their individual agreements. Moreover, the exact text of the provision on Safeguards Rule compliance as it would currently appear in an institutional PPA is not generally available online. In contrast, FSA does provide a sample version of the SAIG enrollment form (i.e., the SAIG agreement) online with its breach provision.\(^9\) It does not, however, provide examples of the prior versions of either provision as they appear in still-operative SAIG agreements or PPAs.

Given that the specific text of the current PPA provision on GLBA Safeguards Rule compliance is not publicly available, we must refer to the Federal Student Aid Handbook with Active Index, 2017–2018,\(^10\) to assess what it likely requires, noting again that different institutional PPAs may contain different versions of this provision based on their effective dates. The text on the Safeguards Rule within the 2017–18 Handbook found at “Volume 2—School Eligibility and Operations 2017–2018: Chapter 7—Record Keeping, Privacy & Electronic Processes” (pp. 2-201–2-202) mirrors the information provided in FSA’s 2016 Dear Colleague Letter, so we assume the Handbook text now serves as the relevant reference since it is more current. We assume the same for the compliance letters, which refer to the older 2016–17 Handbook.

We believe the key references from the 2017–18 Handbook indicating the likely content of the current PPA Safeguards Rule provision read as follows: \(^11\)

**Reporting security breaches to students and the Department**

Schools are strongly encouraged to inform their students of any breaches of security of student records and information. Schools’ SAIG Agreement includes a provision that they must immediately notify FSA at CPSSAIG@ed.gov when there is such a breach. The Department considers any breach to the security of student records and information as a demonstration of a potential lack of administrative capability.

---


Under their Program Participation Agreement (PPA) and the Gramm-Leach-Bliley Act (Public Law 106-102), schools must protect student financial aid information, with particular attention to information provided to institutions by the Department or otherwise obtained in support of the administration of the federal student financial aid programs.

In terms of the SAIG agreement, a review of the copy available on the FSA website shows that it contains two references to “breach”:

1. In a section delineating the responsibilities of the institution’s destination point administrator (DPA) established by the agreement, the text states the DPA must ensure that all Federal Student Aid applicant information is protected from access by or disclosure to unauthorized personnel. In the event of an unauthorized disclosure or breach of applicant information or other sensitive information (such as personally identifiable information), the DPA must immediately notify Federal Student Aid at CPSSAIG@ed.gov.  

2. In a part of the agreement that discusses the responsibilities of the U.S. Department of Education (ED) in responding to a data breach, the text states:

   **Disclosure in the Course of Responding to a Breach of Data.** The Department may disclose records to appropriate agencies, entities, and persons when (a) the Department suspects or has confirmed that the security or confidentiality of information in this system has been compromised; (b) the Department has determined that as a result of the suspected or confirmed compromise, there is a risk of harm to economic or property interests, identity theft or fraud or harm to the security or integrity of the system or other systems or programs (whether maintained by the Department or another agency or entity) that rely upon the compromised information; and (c) the disclosure made to such agencies, entities, or other persons is reasonably necessary to assist in connection with the Department’s efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.  

**Purported FSA Compliance Requirements**

---

It is not clear that FSA’s effort to establish breach notification and information security reporting requirements through the provisions discussed above reflects an appropriate exercise of regulatory authority. Given the range of issues FSA has thus far sought to cover via those provisions, we believe FSA, institutions, and our shared stakeholders (e.g., students and their families) would be better served by addressing breach notification and information security reporting through established collaborative processes, such as negotiated rule-making. In the interim, though, a review of the context surrounding the FSA breach notification and Safeguards Rule compliance provisions indicates that they do not support requirements for institutional reporting of breaches or suspected breaches unrelated to federal student financial aid data, or of suspected breaches of such data, however “suspected” is defined.

The focus of Safeguards Rule compliance with respect to the PPA, at least based on the 2017–18 Handbook, is clearly on student financial aid data; that is appropriate given the Safeguards Rule’s emphasis on customer information, with the customers in this case being students and/or their families seeking federal financial aid. The interpretation of the Handbook’s guidance as focused on FSA data is supported not just by the text quoted previously but also by other references in the section to “student information” and “student records and information” specifically in relation to FSA programs. Thus, it is not clear on what basis FSA asserts authority to require institutional reporting of all breaches or suspected breaches regardless of whether they entail FSA data. Other data collections (e.g., general employee information) would not entail “customer information” relevant to Safeguards Rule compliance within FSA’s scope.

Given the comprehensive review of institutional information security that FSA asserts must accompany breach notification reports, this overly expansive interpretation of its breach notification authority appears to serve as the basis for essentially auditing institutional compliance with the Safeguards Rule (a) in excess of the pending federal single audit objective and (b) in the absence of any officially documented contractual or regulatory compliance framework. For example, we understand that there are no breach notification provisions in the various executed versions of the PPA. They contain at most a reference to an SAIG agreement breach notification provision.

Turning to the SAIG agreement, FSA’s 2015 Dear Colleague Letter states that the agreement requires institutions to notify FSA immediately “in the event of an unauthorized disclosure or an actual or suspected breach of applicant information or other sensitive information (such as PII).” Yet, the SAIG agreement that FSA makes publicly available, which we presume is the

---

14 It is important to remember that the Federal Trade Commission remains the regulator of record for higher education institutions in relation to Safeguards Rule compliance; any potential compliance framework tied to FSA’s contractual provision, which is in turn tied to FSA data, would need to account for FTC oversight and requirements.

15 Runcie and Mitchell, “Protecting Student Information.”
basis for the assertions of possible enforcement actions related to suspected breaches, does not support the letter’s statement. That version of the agreement makes no mention of an institutional requirement to report suspected breaches to FSA. Again, it states: “In the event of an unauthorized disclosure or breach of [Federal Student Aid] applicant information or other sensitive information (such as personally identifiable information), the DPA must immediately notify Federal Student Aid at CPSSAIG@ed.gov.”16

Thus, based on all official, publicly available documentation and guidance, both the PPA and the SAIG agreement confine their statements about GLBA Safeguards Rule compliance and breach notification to FSA data. Likewise, the SAIG agreement provision requiring institutions to immediately report breaches of federal student financial aid data does not refer to “suspected breaches.” The only place in the agreement that addresses suspected breaches discusses FSA’s right to “disclose records to appropriate agencies, entities, and persons” if FSA suspects or confirms a breach of SAIG or related FSA systems.17 The only other potentially relevant reference concerns the requirement that institutional users granted access to the gateway and related systems by the DPA must report suspected compromises of login information, such as a lost or inadvertently shared password, to the DPA.18 Again, neither section mentions a requirement for institutional reporting of suspected student financial aid data breaches to FSA, much less of breaches or suspected breaches not directly related to FSA data.

Official Compliance Documentation and Processes

Institutional confusion about the scope and basis of the authority FSA asserts is exacerbated by a lack of what colleges and universities would generally recognize as official compliance documentation and processes. As mentioned previously, for example, the key terms of the Safeguards Rule provision in the PPA and the breach notification provision in the SAIG agreement are not defined in those agreements or departmental regulations. This creates the potential for significant compliance disconnects between FSA and institutions in relation to the interpretation and application of those provisions. Without a shared understanding of key terms, established by law, regulation, or contract, what constitutes a “breach” and “immediate” notification may be interpreted in subjective and diverging ways, leading FSA to assert a compliance failing where an institution may reasonably determine no such failing exists.

This is particularly problematic when it comes to the assertion of a requirement that institutions must report “suspected breaches.” Any FSA determination of an institutional compliance failure related to a “suspected breach” might easily be seen as arbitrary and

capricious without a shared, consensus-based understanding of what constitutes a “suspected breach” warranting a report to FSA “on the day of detection” (the unofficial definition of “immediate” per statements by FSA officials in conference and webinar presentations).

Returning to the definition of “breach,” the unofficial definition presented by FSA officials has been “the unauthorized disclosure, misuse, alteration, destruction or other compromise of such information,” which is taken from the text of the Safeguards Rule at 16 CFR 314.4(b).\textsuperscript{19} It is important to note, though, that this is part of a section of the Safeguards Rule discussing risk assessment—it is not the Safeguards Rule definition of “breach,” as the rule doesn’t formally define the term.\textsuperscript{20} There are several clauses within the Safeguards Rule, and indeed within the text of GLBA itself, from which one could infer a breach definition. FSA appears to be choosing an inferred definition that supports the broad breach notification requirement it is asserting.

Major federal financial services regulators (e.g., the Federal Reserve, the Federal Deposit Insurance Corporation), however, drew on the language of GLBA itself to infer a definition of “breach” in the context of GLBA compliance for the financial institutions they oversee.\textsuperscript{21} That definition is the “unauthorized access to or use of customer information that could result in substantial harm or inconvenience to a customer.”\textsuperscript{22} (Note that the Safeguards Rule includes the same text in referencing GLBA on standards for safeguarding customer information.)\textsuperscript{23}

Why is this distinction important? It matters because the definition in the official interagency guidance of financial industry regulators provides for a clear breach notification standard:

> When a financial institution becomes aware of an incident of unauthorized access to sensitive customer information, the institution should conduct a reasonable investigation to promptly determine the likelihood that the information has been or will be misused. If the institution determines that misuse of its information about a customer has occurred or is reasonably possible, it should notify the affected customer as soon as possible. Customer notice may be delayed if an appropriate law enforcement agency determines

\begin{itemize}
  \item \textsuperscript{20} Note that the FTC, the oversight authority for higher education GLBA Safeguards Rule compliance, has not issued an official interpretation of the word “breach.”
  \item \textsuperscript{21} 15 USC § 6801(b)(3); available from Cornell Law School, Legal Information Institution, https://www.law.cornell.edu/uscode/text/15/6801.
\end{itemize}
That notification will interfere with a criminal investigation and provides the institution with a written request for the delay. However, the institution should notify its customers as soon as notification will no longer interfere with the investigation. 24 (emphasis added)

Whether this standard, as well as the interagency guidance as a whole, would fit well within the student financial aid context is something that FSA and relevant higher education experts should discuss. Asserting a purported definition or blindly applying guidelines developed for major financial institutions to colleges and universities may not serve FSA, higher education institutions, or their stakeholders well. This notification standard, however, has the benefit of reflecting the intent of GLBA to rest discretion in planning, developing, implementing, and managing information security processes in the hands of covered entities based on, as the Safeguards Rule states, “your size and complexity, the nature and scope of your activities, and the sensitivity of any customer information at issue.”25

Considering how those factors may vary across institutions, from community colleges to large research institutions, it would be appropriate for FSA to work with higher education experts to develop official standards, guidance, and processes that reflect this diversity. ED has a long history of collaborating with the higher education community via negotiated rule-making to develop regulations and/or guidance, as well as related processes, that as a result work more effectively in practice without being unduly burdensome. As previously stated, following long-standing rule-making practices would also provide a clearer, more broadly understood basis for FSA’s efforts to exercise authority in this space than the unilateral introduction of terms.

Furthermore, collaboration between FSA and key stakeholders, such as higher education information security leaders, could help determine the resources, information, and delivery channels regarding security and breach notification compliance that institutions would find most useful. FSA engagement with the higher education IT community is still relatively new, and student financial aid administrators remain FSA’s initial contacts for data issues (see the DPAs). Convening a working group to map FSA, student financial aid, and information security processes and define the terms, guidelines, and resources that would help them function together effectively would likely produce significant advances across shared concerns.

The FSA Cybersecurity Compliance page provides many references and resources, for example, but it does not address this array of issues in a structured, comprehensive fashion. EDUCAUSE would argue that FSA would be hard-pressed to do so in the absence of effective collaboration with higher education professionals. While there are many potential points for discussion and collaborative resolution, a joint effort might address:

- Clarifying the legal and regulatory basis for FSA breach notification and information security reporting requirements, including the appropriate vehicle (e.g., regulation as compared to contractual terms) through which to exercise any relevant authority
- Evaluating the costs and benefits of different notification/reporting options to identify the most cost-effective paths to achieving appropriate levels of compliance
- Integrating FSA’s risk assessment framework for its data and systems with institutional risk assessment approaches to ensure both reflect shared needs and concerns
- Creating a process through which institutions can quickly and effectively validate FSA compliance notifications and related reporting requests
- Establishing secure mechanisms for breach notification and security program reporting when warranted, including secure FSA storage for such information
- Determining whether other official points of contact in addition to the DPA should be included in the SAIG agreement to facilitate information security outreach

**Conclusion**

All sectors of our society face significant information security challenges. Higher education is no exception. Colleges and universities take those challenges very seriously and continue to make substantial, ongoing investments to meet them. We know the same is true of FSA, and we share with you a vital interest in the security and integrity of federal student financial aid data. The trust invested in us collectively by students and their families demands that we work together to minimize the potential for harmful misuse of the data they provide. At present, though, we lack a shared understanding of FSA’s scope of authority for institutional information security and breach notification, the legal and regulatory basis for it, and how best to define and convey relevant compliance requirements and processes. EDUCAUSE urges FSA to work with higher education information security leaders, student financial aid administrators, and other key higher education communities to achieve a consensus-based resolution to these concerns.

---

In the interim, we request that FSA carefully assess its existing approach to information security compliance, and particularly to breach notification. We believe FSA should begin by ensuring that the grounds for initiating such actions are accurately reflected in institutional PPAs and SAIG agreements. We also believe that FSA should utilize the primary institutional contacts already created by its SAIG agreements (i.e., the DPAs) to work with an institution to verify the legitimacy of any breach concerns before proceeding to compliance actions. A key element of this should be to establish whether the institution has confirmed a breach of federal student financial aid data likely to produce substantial harm or inconvenience to students or their families, which would trigger the SAIG notification requirement. Even then, such a requirement should allow room for limitations on information sharing resulting from law enforcement requests, given that state and federal law enforcement agencies may already have active investigations underway. Any formal compliance letters FSA finds it necessary to send should provide sufficient details about the alleged incident to ensure a common frame of reference and facilitate further institutional investigation and response. Formal, standardized processes for the receipt of institutional notifications and reports that account for the sensitivity and confidentiality of such information should also be in place.

Thank you for the opportunity to share our thoughts and concerns about how best to strengthen the important information security relationship between higher education institutions and FSA. EDUCAUSE looks forward to working with FSA and our higher education colleagues to achieve the clarity and consensus such an effort requires.

Sincerely,

Jarret S. Cummings
Director, Policy and Government Relations
EDUCAUSE

Cc: Matthew Sessa, Deputy Chief Operating Officer, Federal Student Aid, U.S. Department of Education

Tiina K.O. Rodrigue, Senior Advisor–Cybersecurity, Federal Student Aid, U.S. Department of Education