



Office of the President

October 9, 2001

*BY HAND DELIVERY*

Donald S. Clark, Esq.  
Secretary  
Federal Trade Commission  
Room 159  
600 Pennsylvania Avenue, NW  
Washington, DC 20580

**Re: Gramm-Leach-Bliley Act Privacy Safeguards Rule, 16 C.F.R. Part 314—Comment**

Dear Mr. Clark:

On behalf of the American Council on Education ("ACE") and the other national higher education associations listed below, I submit these comments on the Federal Trade Commission's ("FTC") proposed rule regarding administrative, technical, and physical information safeguards for customer records of financial institutions ("the Safeguards Rule") that the FTC intends to promulgate under Title V of the Gramm-Leach-Bliley Act ("the GLB Act"), Pub. L. No. 106-102 (*codified at* 15 U.S.C. § 6801 *et seq.*). *See* 66 Fed. Reg. 41162 (2001). In its proposed rule, the FTC specifically sought public comments regarding "whether and how compliance with . . . other laws and rules relating to information security . . . should be addressed in the proposed rule." *Id.* at 41164.

ACE represents all sectors of American higher education. Founded in 1918, it is a non-profit national education association whose members include more than 1,800 public and private colleges, universities, and educational organizations throughout the United States. As a leading participant in higher education affairs, ACE's purpose is to promote the interests of all members of the academic community, including students and their parents. ACE members participate in various federal, state, and institutional student financial aid programs, including student loan and grant programs. It is apparently such programs that the FTC viewed as "financial activities" that may cause colleges and universities to be treated as "financial institutions" under the GLB Act. *See* 65 Fed. Reg. 33646, 33648 (May 24, 2000).

Higher education institutions have a fundamental interest in the integrity of education records and have been subject to federal law concerning the privacy of education records since 1974. We respectfully request that the Safeguards Rule provide that higher education institutions that comply with the Family Educational Rights and Privacy Act ("FERPA"), 20 U.S.C. § 1232g, and its implementing regulations, 34 C.F.R. pt. 99, shall be deemed in compliance with the Safeguards Rule. The FTC has already recognized in its earlier rule under Title V ("the Privacy Rule") that compliance with FERPA satisfies the GLB Act's privacy provisions. *See* 16 C.F.R. § 313.1(b). We submit that it is similarly unnecessary, and would be duplicative and burdensome, to require higher education institutions already in compliance with FERPA to comply separately with the Safeguards Rule.

1. JUST AS THE FTC SOUNDLY CONCLUDED THAT COMPLIANCE WITH FERPA SATISFIES THE GLB ACT'S PRIVACY PROVISIONS, THE FTC SHOULD CONCLUDE THAT FERPA COMPLIANCE SATISFIES THE SAFEGUARDS RULE.

In the Privacy Rule the FTC concluded that compliance with FERPA satisfied the GLB Act's privacy requirements. *See id.* Because the FTC recognized that higher education institutions are already subject to "stringent privacy provisions" under FERPA, 65 Fed. Reg. 33646, 33648 (May 24, 2000), the Privacy Rule specifically provided that "[a]ny institution of higher education that complies with . . . FERPA . . . , 20 U.S.C. § 1232g, and its implementing regulations, 34 CFR part 99, and that is also a financial institution subject to the requirements of this part, shall be deemed to be in compliance with this part if it is in compliance with FERPA." *Id.* at 33678. As described below, FERPA imposes similarly stringent safeguards requirements on higher education institutions. Accordingly, the FTC should conclude that compliance with FERPA's rigorous privacy safeguards constitutes compliance with the Safeguards Rule.

First, it would be unnecessary and duplicative to require higher education institutions to comply with the requirements delineated in the proposed Safeguards Rule, for those requirements merely replicate the rigor of the existing FERPA safeguards requirements. For example, the Safeguards Rule would oblige institutions to "requir[e their] service providers by contract to implement and maintain . . . safeguards" to protect the privacy of customer information. 66 Fed. Reg. at 41169. Similarly, FERPA already requires third parties to whom institutions permissibly disclose information under the statute to comply with FERPA's security and privacy requirements. *See* 34 C.F.R. § 99.33.

Moreover, in enacting FERPA, Congress legislatively determined the risks associated with improper disclosure of students' education records and imposed those privacy and safeguards requirements that it deemed warranted to counter those risks.

Specifically, Congress chose to define broadly the "education records" to which FERPA protection applies, *see* 20 U.S.C. § 1232g(a)(4)(A), generally to prohibit disclosure of such records absent prior written consent, *see id.* § 1232g(b), to impose stringent record-keeping requirements to document disclosures pursuant to the statute, *see id.* § 1232g(b)(4)(A), to require third parties to whom information is permissibly disclosed to comply with FERPA's requirements, *see id.* § 1232g(b)(4)(B), and to ensure compliance with FERPA's stringent requirements by providing students with notice of their FERPA rights and the means by which to exercise those rights, *see id.* §§ 1232g(e) (requiring annual notices), (g) (providing for the filing of complaints of alleged FERPA violations), and by authorizing a severe penalty – the loss of federal funding – for failure to comply with FERPA's privacy and safeguard requirements, *see id.* § 1232g(f). It would both contravene legislative intent and be wholly unnecessary to require higher education institutions to conduct a second round of assessments regarding what security and confidentiality to accord student records. Those institutions' compliance with the very extensive security measures imposed by Congress in light of its own risk assessment is sufficient to safeguard students' education records.

2. HIGHER EDUCATION INSTITUTIONS' ONGOING IMPLEMENTATION OF FERPA'S PRIVACY SAFEGUARDS MEETS THE CONCERNS ADDRESSED BY THE SAFEGUARDS RULE.

While the provisions of FERPA, as discussed more fully below, address the objectives of the GLB Act, higher education institutions take their FERPA obligations, which require attention to security concerns, seriously in practice. Compliance procedures include, in the words of the proposed Safeguards Rule, "identify[ing] reasonably foreseeable internal and external risks to the security, confidentiality, and integrity" of education records "that could result in the unauthorized disclosure, misuse, alteration, destruction, or other compromise of such information, and assess[ing] the sufficiency of any safeguards in place to control these risks." 66 Fed. Reg. at 41169.

At most institutions, the registrar is responsible for FERPA compliance in coordination with other campus officials. *See Privacy and the Handling of Student Information in the Electronic Networked Environments of Colleges and Universities* (Cause [now Educause], in cooperation with the American Association of Collegiate Registrars and Admissions Officers, 1997) at 1 ("White Paper"), available at <http://www.educause.edu/issues/privacy.html>. While FERPA establishes strict legal requirements for safeguarding educational records, campus officials regularly review how to implement those safeguards, particularly in electronic networks. *See id.* at 3; *see generally* American Association of Collegiate Registrars and Admissions Officers, *The AACRAO 2001 FERPA Guide* ("FERPA Guide"). The scope of these efforts includes, but

extends far beyond, student financial aid programs that the FTC apparently views as "financial activities" under the GLB Act. *See* 65 Fed. Reg. at 33648. No one knows better than registrars how sensitive educational records are and how important it is to keep them secure. In addition to measures to address electronic security over educational institutions' electronic networks, registrars have long implemented rigorous physical security measures to prevent unauthorized access to educational records. Registrars' security incentives include protecting not only the privacy of records under their control, but also the integrity of those records from alteration either by the subject of the records or others who might wish to alter them. *See generally FERPA Guide; White Paper.*

The American Association of Collegiate Registrars and Admissions Officers ("AACRAO") and Educause, the association of higher education information technology professionals, have provided extensive guidance to higher education institutions and their information technology professionals for compliance with FERPA's privacy safeguards in the context of computer information systems. *See generally White Paper.* This guidance addresses information processing, storage, transmission, and disposal standards and procedures, as well as prevention and response measures for attacks, intrusions, or other system failures. *See id.* at 29-30. It covers development of policies, processes, and procedures to address physical and procedural security issues. *See generally id.* at 27-32. The guidance also discusses designing and implementing safeguards to control identified risks and regularly testing or otherwise monitoring the effectiveness of the safeguards' key controls, systems, and procedures. *See generally id.* In addition, Educause has established a security task force to identify short- and long-term actions to address systems security issues in higher education. *See* Educause, Systems Security Taskforce, at <http://www.educause.edu/security/>. Like the proposed Safeguards Rule, *see* 66 Fed. Reg. at 41163, 41168, AACRAO and Educause recognize that institutions must make an assessment of their own circumstances in order to implement appropriate information privacy procedures: "[H]ow the data will be protected and the measures that are reasonable for the assessed risks are institutional decisions that must be considered in light of the network environment and institutional culture." *White Paper* at 29.

The U.S. Department of Education ("the Department") and higher education associations provide technical assistance to institutions concerning FERPA compliance. Through these higher education associations, colleges and universities assist each other by sharing policies, procedures, and good practices. For example:

- The Department's Family Policy Compliance Office ("FPCO"), which is responsible for administering FERPA, provides guidance regarding statutory and regulatory requirements. *See* FERPA Online Library, at

<http://www.ed.gov/offices/OM/fpco/ferpaonline.html> (providing Internet links to FPCO letters of technical assistance written in response to institutional inquiries). The Department has also prepared a model annual notification of rights under FERPA for use by postsecondary institutions. See 61 Fed. Reg. at 59297.

- Higher education associations such as AACRAO and the National Association of Student Financial Aid Administrators ("NASFAA") sponsor FERPA workshops and publish detailed guidance on FERPA compliance, including procedures to assist higher education institutions in performing self-assessments to ensure compliance with FERPA's privacy and safeguards requirements. See, e.g., *FERPA Guide* § 6.9, at 72-76 (providing a "FERPA Audit" to assess institutional compliance with statutory and regulatory requirements, including with respect to security policies and protocols, training, and accountability); NASFAA, *Self-Evaluation Guide for 1999-2000 and 2000-2001*, at IV-1, available at <http://www.nasfaa.org/PDFs/2001/FERPA.pdf>.
- In conjunction with AACRAO, Educause published a White Paper, discussed above, in 1997 on proper safeguards for student information in college and university electronic networked environments. See *White Paper*. Educause distributed the White Paper to each of its members and has posted the White Paper on its website.
- The Department, NASFAA, AACRAO, the National Association of College and University Business Officers ("NACUBO"), and other higher education associations were founding members of the Postsecondary Electronic Standards Council ("the PESC"), an organization intended to support the development of national electronic standards for the higher education community. See PESC, *Frequently Asked Questions*, at <http://www.standardscouncil.org/faqright.htm>. In conjunction with the PESC and others, AACRAO, through its standing committee for the Standardization of Postsecondary Education Electronic Data Exchange, has developed a number of standards, approved for trial use by the American National Standards Institute Accredited Standards Committee x12, regarding electronic data interchange, including with respect to data encryption techniques to improve the confidentiality of student information. See *FERPA Guide* § 5.11, at 21-22; see also PESC, *Standards*, at <http://www.standardscouncil.org/>.

- Colleges and universities assist one another in formulating strategies to safeguard student records, including through the submission of examples of such strategies to the AACRAO and Educause websites. Those associations collect and post effective practices and solutions relating to universities' use and management of information technology. See AACRAO, Resource Center Index, at [http://www.aacrao.org/resource\\_center/rcindex.htm](http://www.aacrao.org/resource_center/rcindex.htm); Educause, Effective Practices and Solutions, at <http://www.educause.edu/ep/>; Educause, Information Resources Library, at <http://www.educause.edu/ir/ir-library.html>.

These resources, utilized in the context of very extensive guidance from the Department, facilitate substantial employee training and management for implementation of FERPA's privacy safeguards.

As a result of these and similar intensive efforts to meet FERPA's requirements, the Department has never had cause to withhold, and has never withheld, federal funding from a higher education institution for failure to comply with FERPA. In light of FERPA's comprehensive and rigorous privacy safeguards and institutions' established and ongoing compliance procedures, it is unnecessary to require higher education institutions already in compliance with FERPA to comply with the Safeguards Rule.

3. HIGHER EDUCATION INSTITUTIONS ARE ALREADY SUBJECT TO STRICT PRIVACY SAFEGUARDS UNDER FERPA.

Compliance with FERPA should satisfy the Safeguards Rule because, as ACE explained in its comments on the Privacy Rule, FERPA already requires higher education institutions to comply with strict privacy safeguards that serve the GLB Act's objectives. See Letter from S. Ikenberry to D. Clark (Oct. 10, 2000). Those objectives include ensuring "the security and confidentiality of customer records," protecting against "anticipated threats or hazards to the security or integrity of such records," and preventing "unauthorized access to or use of [customer] records." 66 Fed. Reg. at 41162 (citing the GLB Act, 15 U.S.C. § 6801(b)(1)-(3)).

*Ensuring Security and Confidentiality.* FERPA applies to "education records," which are broadly defined to include any records "(1) Directly related to a student; and (2) Maintained by an educational agency or institution or by a party acting for the agency or institution." 34 C.F.R. § 99.3; see also 20 U.S.C. § 1232g(a)(4)(A). FERPA promotes the security and confidentiality of education records in several ways.

First, FERPA strictly limits disclosures of such records by generally requiring the student's written consent before the release to third parties of education records or

personally identifiable information contained therein. *See* 20 U.S.C. § 1232g(b)(1); 34 C.F.R. § 99.30. Moreover, for such consent to be valid, it must be signed and dated, and must specify the records to be disclosed, the purpose of the disclosure, and the party to whom the disclosure may be made. *See* 34 C.F.R. § 99.30(b). Even with respect to disclosures to school officials, including professors, within an institution of higher education, FERPA requires the institution to determine whether the school official has a legitimate educational interest in the information before any such disclosure, *see id.* § 99.31(a)(1), and to specify in an annual notice to students the specific criteria by which such a determination will be made, *see* 34 C.F.R. § 99.7(a)(3)(iii). *See also* 61 Fed. Reg. 59291, 59297 (Nov. 21, 1996) (model annual notice describing “legitimate educational interest”); *White Paper* at 24, 40 (discussing definition of “legitimate educational interest” in school policies).

FERPA also protects the security and confidentiality of education records by requiring an annual notice, referenced above, to inform students of their privacy rights. *See id.* § 99.7(a). In addition, by granting students a right to file a complaint with the Department in the event of a perceived FERPA violation, *see id.* § 99.63, FERPA provides an administrative process for holding institutions of higher education in compliance with the statute’s privacy safeguards requirements. Similarly, FERPA provides a severe penalty for failure to comply with its provisions – the potential loss of, and even termination of eligibility for, federal funding. *See id.* § 99.67(a).

*Protecting Against Anticipated Threats or Hazards to Security or Integrity.* FERPA contains numerous safeguards to protect the security and integrity of student records. As described above, FERPA prohibits the disclosure of such records without prior written consent or other legitimate justification. *See* 20 U.S.C. § 1232g(b); 34 C.F.R. §§ 99.30-99.31. Moreover, an institution may not release information to third parties except “on the condition that the party to whom the information is disclosed will not disclose the information to any other party without the prior consent of the parent or eligible student.” 34 C.F.R. § 99.33(a)(1). FERPA thus imposes the same stringent security requirements on third parties to whom information is disclosed pursuant to the statute. *See id.* § 99.33.

In addition, FERPA protects the integrity of education records by granting students a right to inspect and review their education records. *See id.* § 99.10(a). If the student concludes that the records contain inaccurate or misleading information or violate the student’s right to privacy, he or she may ask the institution to amend the record. *See id.* § 99.20. Moreover, if the institution does not amend the record as requested, it must grant the student a hearing, conducted in accordance with FERPA-specified requirements, to challenge the content of the student’s record. *See id.* §§ 99.21 (hearing rights), 99.22 (hearing conduct requirements). If, after the hearing, the

institution still decides not to amend the student's record, the student has a right to place a statement in the education record commenting on the contested information and the institution's decision. *See id.* § 99.21(b)(2). The institution must maintain this statement with the contested part of the record for as long as the record is maintained, and must disclose the statement whenever it discloses the contested part of the record. *See id.* § 99.21(c).

*Preventing Unwarranted Access and Use.* FERPA prohibits unwarranted access and use of student records. As described above, institutions must obtain detailed written consent before releasing personally identifiable information. *See id.* § 99.30. Institutions that release information to third parties as permitted under FERPA must ensure that the recipient complies with FERPA, and the recipient may use the information only for the purposes for which the disclosure was made. *See id.* § 99.33. Even with respect to disclosures to other officials within a higher education institution, FERPA requires a specific determination of those officials' legitimate educational interests in the information requested, *see id.* § 99.31(a)(1), and requires that this determination be made in accordance with previously established, published criteria, *see id.* § 99.7(a)(3)(iii).

FERPA also protects against unauthorized use of or access to education records by ensuring that students are aware of their right to privacy in those records, *see id.* § 99.7(a)(2)(iii) (delineating the need for consent prior to disclosure of student education records), and by requiring institutions to document each request for, or disclosure of, a student's records pursuant to the statute, *see id.* § 99.32(a)(1). Where an institution has permissibly disclosed information to a third party with the understanding that that third party may re-disclose the information on the institution's behalf, FERPA's record-keeping requirements also require institutions to specify the additional parties to which the third party may permissibly disclose the information and the legitimate interests each of these additional parties has in the requested information. *See id.* § 99.32(b).

4. THE FTC SHOULD CONFIRM IN THE FINAL REGULATIONS THAT COMPLIANCE WITH FERPA SATISFIES THE REQUIREMENTS OF THE SAFEGUARDS RULE.

As FTC Chairman Muris's recent remarks at the Privacy 2001 Conference indicate, the FTC has a substantial and wide-ranging privacy agenda. Because higher education institutions are already covered by FERPA, we respectfully submit that the FTC can most effectively devote its resources to oversight of sectors where privacy is not already regulated by another federal agency.

For the foregoing reasons, we respectfully request that, consistent with the FTC's Privacy Rule, the FTC confirm in its final Safeguards Rule that compliance with FERPA satisfies the Safeguards Rule's requirements. We suggest that the FTC include in the



Safeguards Rule the same statement that is included in the Privacy Rule regarding compliance with FERPA.

We appreciate your consideration of these comments. Please call me if you have any questions or need additional information.

Sincerely,



David Ward  
President

DW/cms

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 Jesuit Colleges and Universities  
Council for Advancement and Support of Education  
Council of Independent Colleges  
National Association for Equal Opportunity in Higher Education  
National Association of State Universities and Land-Grant Colleges  
National Association of Student Financial Aid Administrators  
United Negro College Fund