



NACUALERTS

May 16, 2003

Vol. 1 No. 4

TOPIC:

FTC'S GRAMM-LEACH-BLILEY ACT SAFEGUARDS RULE: GUIDELINES FOR COMPLIANCE

Colleges and Universities should be aware of a Federal Trade Commission (FTC) rule that will affect their record-keeping practices and procedures, especially with respect to student financial aid records. The FTC's [Safeguards Rule](#) promulgated under the [Gramm – Leach – Bliley Act](#) ("GLBA") goes into effect on May 23, 2003 and is aimed at ensuring the safeguarding and confidentiality of customer information held in the possession of covered "financial institutions." The Safeguards Rule requires all covered financial institutions to have in place by May 23, a written information security program designed to:

- (i) ensure the security and confidentiality of customer records,
- (ii) protect against any anticipated threats or hazards to the security of such records, and
- (iii) protect against the unauthorized access or use of such records or information in ways that could result in substantial harm or inconvenience to customers [\[1\]](#).

The FTC has made it clear that it considers educational institutions to be "financial institutions" subject to its jurisdiction for purposes of GLBA [\[2\]](#). Further, unlike the FTC's earlier [GLBA Privacy Rule](#), the Safeguards Rule contains no exemption for institutions that are subject to the Family Educational Rights and Privacy Act (FERPA). As a result, educational institutions that engage in financial institution activities as defined in the Act, such as processing student loans, are required to comply with the Safeguards Rule by May 23. This summary provides a brief overview of the Safeguards Rule, describes some of the major issues relating to compliance with the Rule, and includes an outline for creating a compliant written information security program.

DISCUSSION:

The Safeguards Rule requires each covered institution to develop, implement and maintain a "comprehensive information security program" that is "written in one or more readily accessible parts", and that includes "administrative, technical and physical safeguards" designed to accomplish the objectives described above [\[3\]](#). The Safeguards Rule expressly recognizes that each institution's information security program may vary, based on its size and complexity, the nature and scope of its activities, and the sensitivity of the customer information at issue [\[4\]](#). Institutions that fail to comply with the Safeguards Rule may be subject to FTC enforcement actions, which can result in consent decrees and the imposition of fines or other penalties. In addition, to the extent the Safeguards Rule is interpreted as

imposing a general duty on educational institutions to safeguard covered financial information, it may prove relevant in actions brought under general negligence law theories in response to failures to maintain the confidentiality of such information.

ELEMENTS

In order to “develop, implement and maintain” the required written information security program, the Safeguards Rule requires each institution to:

- § designate one or more employees to coordinate the program;
- § identify “reasonably foreseeable” internal and external risks to the security and confidentiality of customer information that could lead to unauthorized disclosure, use, alteration, destruction or other compromise of such information and “assess the sufficiency” of the institution’s safeguards in place to control these risks. Such risk assessment must include, at a minimum, risks in areas of operation such as:
 - § employee training and management,
 - § information systems, and
 - § detecting, preventing, and responding to attacks against the institution’s systems;
- § implement safeguards to manage the identified risks and regularly test or monitor such safeguards;
- § oversee the institution's service providers by:
 - § selecting and retaining service providers that are capable of maintaining appropriate safeguards for the customer information at issue, and
 - § requiring service providers by contract to implement and maintain such safeguards; and
- § evaluate and adjust the institution's security program in light of such risk assessment, any material change to institutional business operations or any other circumstances that may have a material impact on the institution's information security program [\[5\]](#).

PRACTICAL CONSIDERATIONS AND ISSUES:

- § **Scope.** The most difficult challenge in interpreting the Safeguards Rule and in implementing a compliant written information security program lies in identifying the scope of information and activities covered by the rule. The Safeguards Rule expressly applies to all “customer information” in the possession of an institution. The term “customer information” is defined under the rule as any record containing “nonpublic personal information” (as defined in the FTC’s Privacy Rule under GLBA), whether in paper, electronic or other form, that is handled or maintained by or on behalf of the institution or its affiliates, about a “customer” of that institution. Under the FTC’s GLBA Privacy Rule, the term “nonpublic personal information” includes “personally identifiable information,” which in turn is defined as any information:

- (i) a consumer provides to obtain a financial product or service from the institution,
- (ii) about a consumer resulting from any transaction with the institution involving a financial product or service, or
- (iii) otherwise obtained about a consumer in connection with providing a financial product or service to that consumer."[\[6\]](#)

Based on the foregoing, it may be possible for institutions to take the position that their obligations under the Safeguards Rule, including the scope of their written information security program, apply only to information collected or maintained in connection with the institution's financial institution activities – *i.e.*, most notably their student financial aid related activities. As a practical matter, however, it may be difficult for institutions to segregate information that is collected in connection with financial institution related activities (such as Social Security numbers) from other information maintained with respect to its student population. Therefore, prior to implementing a narrow interpretation of the Safeguards Rule's requirements, institutions should carefully evaluate whether they wish to apply different security standards to potentially overlapping sets of student records information.

§ **Drafting Suggestions.** In drafting an institution's information security program, it is important to note that the FTC's rules are intended to be flexible in order to take into account the size and complexity of the institution and the nature and sensitivity of the information that is collected. Less stringent information security standards may be appropriate for information that is less sensitive. In addition, the FTC's rules expressly recognize that an institution's information security program may be maintained in one or more documents. Thus, it should be possible to incorporate existing policies and procedures relating to the safeguarding of information and to the proper use of institutional network resources, such as existing acceptable use, information technology security and student record access policies and procedures.

§ **Risk Management Concerns.** Any institution faced with creating a written information security program required under the Safeguards Rule also should consider the paper trail it creates in adopting and implementing the program. The Safeguards Rule does not require that the written program be made publicly available (although it is possible that the program could be a required disclosure under a state freedom of information act request or through other means). Any documents that are created in the course of developing or implementing the program, and in particular those documents that are created in the course of assessing the risks associated with network vulnerabilities should, if at all possible, be clearly labeled as drafts. Such drafts may be exempt from disclosure under freedom of information statutes or protected under the attorney client privilege. Treating in this manner any preliminary drafts created in connection with the process of assessing vulnerabilities and developing and implementing a comprehensive information security program should help to shield them from later discovery pursuant to public records information requests or in the course of private litigation.

SUGGESTED OUTLINE OF COMPREHENSIVE INFORMATION SECURITY PROGRAM:

A suggested policy outline for use in creating a GLBA-compliant information security program is available [here](#). As noted above, each institution's requirements will vary depending on a number of factors, including the specific nature of its activities and the information that it maintains. Accordingly, this outline is only a suggested beginning point for drafting an institution's information security program and is not intended as formal legal advice.

CONCLUSION:

Although colleges and universities are not perceived as "financial institutions" in the traditional sense (nor students or others as "customers"), the definition of that term under the GLBA regulations has brought a wide range of entities, including colleges and universities, under the jurisdiction of the GLBA Safeguards Rule. To add to the confusion, while educational institutions that are in compliance with FERPA are generally exempt from the FTC's GLBA Privacy Rule, there is no similar exemption afforded educational institutions under the FTC's Safeguards Rule. As a result, colleges and universities that engage in covered activities are required to develop a written information security program, and to otherwise come into compliance with the Safeguards Rule as described in this summary, by the May 23, 2003 deadline established by the FTC. Thereafter, institutions will need to follow through on the obligations undertaken in their policies by regularly testing or monitoring the information safeguards they have established.

[FOOTNOTES](#)

RESOURCES for COUNSEL:

Statutes and Regulations:

§[Gramm-Leach-Bliley Act](#)

§[FTC: Final Rule--Standards for Safeguarding Customer Information \(16 CFR Part 314\)](#)

§[FTC: Final Rule--Privacy of Consumer Financial Information \(16 CFR Part 313\)](#)

Agency Guidance:

§[FTC Guidance: Financial Institutions and Customer Data--Complying with the Safeguards Rule](#)

Other Resources:

§[FTC Standards for Safeguarding Customer Information](#) (Privacy Officer Advisor, July 2002)

§[IT Security for Higher Education: A Legal Perspective](#) (by Peter Cassatt; prepared for the EDUCAUSE/Internet2 Security Task Force)

§[NACUA Cybersecurity Resource Page](#)

§[Catholic University of America Gramm-Leach-Bliley Resources Page](#)

Policies:

§[Catholic University of America Draft Information Security Plan](#)

Websites:

[§International Association of Privacy Professionals](#)

[§Complianceheadquarters.com](#) (Privacy pages)

Authors:

[Peter Cassat, Dow Lohnes & Albertson](#)

[Kenneth Salomon, Dow Lohnes & Albertson](#)

Permitted Uses of NACUANotes and NACUAlerts [Copyright and Disclaimer Notice](#)

[NACUANotes/Alerts Home Page](#) | [NACUANotes/Alerts Issues](#)

[Contact Us](#) | [NACUA Home Page](#)

“To advance the effective practice of higher education attorneys for the benefit of the colleges and universities they serve.”

*National Association of College and University Attorneys
One Dupont Circle N.W., Suite 620, Washington, D.C. 20036
voice: 202.833.8390 – fax: 202.296.8379*