

compliance with the gramm-leach-bliley act's safeguards rules

PROTECTING THE CONFIDENTIALITY of students' information is nothing new for schools. Since the passage of the Family Educational Rights and Privacy Act (FERPA) in 1974, educational institutions have been legally required to ensure the privacy of their students' personally identifiable information.

However, more recent laws and regulations imposing additional compliance obligations have caught many colleges and universities by surprise. In particular, as of May 23, 2003, educational institutions must comply with the Federal Trade Commission's (FTC's) Safeguards Rule, promulgated pursuant to the Gramm-Leach-Bliley Act (GLBA). The GLBA Safeguards Rule obligates institutions to protect certain individually identifiable financial information.

Despite the May implementation date, requirements under this rule continue to leave institutions' administrators and IT directors scrambling to come into compliance.

Yes, the Rule Applies to Schools

As part of its implementation of the GLBA, the FTC originally issued its Safeguards Rule in May 2000, setting forth requirements relating to the administrative, technical, and physical safeguarding of customer records and information. Many institutions have been unsure about whether, and to what extent, the Safeguards Rule applies to colleges and universities. Until recently, some institutions were under the

impression that the FTC's Safeguards Rule did not apply to them at all. According to one practitioner, the education community "really missed the boat on this. As a result, institutions are scrambling to catch up and get their compliance plans in place."

Some of the confusion about the applicability of the Safeguards Rule arose because the FTC traditionally has not exercised jurisdiction over non-profit entities. Under Section 5 of the FTC Act, which gives the FTC the authority to regulate against unfair and deceptive acts and practices, the FTC is only vested with the authority to bring enforcement actions against for-profit entities. In contrast, the GLBA vests the FTC with the author-

ity to use its enforcement tools against any "financial institution," regardless of that institution's for-profit or non-profit nature.

Although colleges and universities are not perceived

as "financial institutions" (nor students as "customers") in the traditional sense, the definition of that term under the GLBA and the FTC's implementing regulations has brought a wide range of entities, including colleges and universities, under the FTC's jurisdiction. The FTC has expressly stated that it considers educational institutions to be "financial institutions" subject to its jurisdiction for purposes of the GLBA because "[m]any, if not all, [educational] institutions appear to be significantly engaged in lending funds to consumers."

Adding to the perception that educational institutions need not concern themselves with the Safeguards Rule is the Department of Education's (ED's) silence on the issue. However, ED does not have jurisdiction to enforce the GLBA and, as a result, has not issued any guidance regarding institutions' obligations under the Safeguards Rule.

Further adding to the confusion, the FTC's earlier GLBA Privacy Rule exempts from its requirements educational institutions that are in compliance with the FERPA, *while the Safeguards Rule affords no similar exemption*. As a result, educational institutions that engage in financial institution activities as defined in the GLBA, such as processing student loans, are required to comply with the Safeguards Rule even if they are exempt from the FTC's earlier GLBA Privacy Rule.

What Is Required?

Under the Safeguards Rule, educational institutions, in their



capacity as “financial institutions,” must have in place a written information security program designed to

1. **ensure** the security and confidentiality of customer records;
2. **protect** against any anticipated threats or hazards to the security of such records; and
3. **protect** against the unauthorized access or use of such records or information in ways that could result in substantial harm or inconvenience to customers.

To comply with these requirements, colleges and universities must 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. 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.

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 and assess the sufficiency of the safeguards in place to control these risks;
- implement safeguards to manage the identified risks and regularly test or monitor such safeguards;
- select and retain service providers that are capable of maintaining appropriate safeguards for the customer information at issue and require 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 and any other circumstances that may have a material impact on the institution’s information security program.

Institutions that fail to comply with the 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 rule is interpreted as imposing a general duty on educational institutions to safeguard student financial information, it may prove

Read More About It

You can find additional information about the Gramm-Leach-Bliley Act at the following URLs:

Guidance on FTC Standards for Safeguarding Customer Information
(NASFAA, August 28, 2003) www.nasfaa.org/publications/2003/rftcandglb082803.html

Colleges and Universities Must Comply by May with FTC’s Information-Protection Rule
(NASFAA, February 25, 2003) www.nasfaa.org/publications/2003/customerinfo022503.html

NACUBO Advisory Report 2003-01: Colleges and Universities Subject to New FTC Rules Safeguarding Customer Information
(National Association of College and University Business Officers, January 13 2003), www.nacubo.org/public_policy/advisory_reports/2003/2003-01.pdf

relevant in actions brought under general negligence law theories in response to failures to maintain the confidentiality or security of personal information.

Which Data Are Covered?

One of the key challenges in determining how to comply with the FTC’s Safeguards Rule lies in distinguishing between financial records that are covered by the rule and other student data that are not covered. The Safeguards Rule incorporates a complicated definition of “customer information” that

is subject to the rule and expressly encompasses all “customer information” in the possession of an institution. Under the FTC regulations, the term “customer information” is defined as any record containing “non-public personal information” (as defined in the FTC’s Privacy Rule under GLBA) about a customer of that institution—whether in paper, electronic, or other form—that is handled or maintained by or on behalf of the institution or its affiliates.

Under the FTC’s GLBA Privacy Rule, the term “nonpublic personal information” includes “personally identifiable information,” which 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.”

Based on the foregoing, it may be possible for institutions to take the position that the Safeguards Rule applies only to information actually collected or maintained in connection with the institution’s financial institution activities—e.g., student financial aid-related activities. As a practical matter, however, it may be difficult for institutions to segregate information (such as Social Security numbers) collected in connection with financial institution-related activities from other student information. In fact, faced with this dilemma, some institutions are electing to treat all personally identifiable student information as subject to the Safeguards Rule

Practical Considerations for Schools

Regardless of the precise approach an institution ultimately takes with respect to the treatment of its covered customer information, it is helpful to keep in mind a number of practical considerations.

COMPLIANCE WITH THE GRAMM-LEACH-BLILEY ACT


BY PETER CASSAT



1. The most important step is for the institution to put into place its written information security program. As noted earlier, the FTC's rules expressly contemplate that each institution's program may vary based on such factors as its size and complexity and the sensitivity of the information at hand.
2. In drafting the required information security program, it is helpful to keep in mind that the FTC rules also expressly recognize that the program may be contained in one or more separately maintained 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. Examples include existing acceptable use, information technology security, and student record access policies and procedures.

3. Finally, in carrying out the risk assessment and mitigation activities mandated by the Safeguards Rule, colleges and universities should be sensitive to the potentially harmful nature of any records generated along the way. Even informal records that identify potential vulnerabilities, such as e-mails and meeting agendas, may be damning in the hands of would-be hackers or plaintiff's attorneys. As a result, institutions should seek to preserve the confidential nature of these records to the greatest extent possible.

In this regard, in promulgating its Safeguards Rule, the FTC expressly noted that an institution's written information-security program need not be made publicly available. Nevertheless, institutions should be aware that their written programs and related documentation may be subject to dis-

covery pursuant to state open records laws or in connection with litigation. As a result, all drafts and deliberative documents relating to the creation and implementation of the program should be labeled as such and, to the extent applicable, subject to the attorney-client privilege. 

Peter Cassat is a member of the law firm of Dow, Lohnes & Albertson and specializes in the areas of intellectual property, information technology and privacy law. He can be reached at pcassat@dowlohn.com or by telephone at (202) 776-2724.

Legal Checkup is *Transcript's* regular feature on the legal issues affecting financial aid professionals and their institutions. The article should not be considered legal advice. For legal questions relating to the Gramm-Leach-Bliley Act or related issues, contact an attorney familiar with your institutions' circumstances.