NACUBO
Advisory Report 2003-01

January 13, 2003

Colleges and Universities Subject to New FTC Rules Safeguarding Customer Information

Colleges and universities have until May 2003 to be in compliance with a recent Federal Trade Commission (FTC) rule related to the safeguarding of customer financial information. The rules require financial institutions, including colleges and universities, to develop plans and establish policies to protect such information. This report summarizes the safeguarding rules.

Background

The regulations under 16 CFR Part 314, published in May 2002 (May 23 *Federal Register*, p. 346484), stem from the Gramm-Leach-Bliley Act (the GLB Act or the Act) which was enacted in 2000 to repeal Depression-era restrictions prohibiting banks from engaging in "risky" financial practices under the Glass-Steagall Act. These restrictions have now been lifted in a way that will permit the creation of "one-stop financial services supermarkets," in which a variety of financial services can be offered.

The law also mandates extensive new privacy protections for consumers. The GBL Act requires financial institutions to take steps to ensure the security and confidentiality of customer records such as names, addresses, phone numbers, bank and credit card account numbers, income and credit histories, and Social Security numbers.

The GBL Act broadly defines "financial institution" as any institution engaging in the financial activities enumerated under the Bank Holding Company Act of 1956, including "making, acquiring, brokering, or servicing loans" and "collection agency services." Because higher education institutions participate in financial activities, such as making Federal Perkins Loans, FTC regulations consider them financial institutions for GLB Act purposes.

The GLB Act spells out several specific requirements regarding the privacy of customer financial information. Following passage of the Act, NACUBO and other higher education associations worked to have colleges and universities exempted from the jurisdiction of FTC because they did not fit the typical definition of a financial institution under the GLB Act. As a result, under regulations promulgated in May 2000, colleges and universities are deemed to be in compliance with the *privacy* provisions of the GLB Act if they are in compliance with the Family Educational Rights and Privacy Act (FERPA). However, higher education institutions are subject to the provisions of the Act related to the administrative, technical, and physical *safeguarding* of customer information.

General Standards for Safeguarding Customer Information

Financial institutions, including colleges and universities, must meet a general standard in order to comply with the "to develop, implement, and maintain a comprehensive written information security program that contains administrative, technical, and physical safeguards" appropriate to the size and complexity of the institution, the nature and scope of its activities, and the sensitivity of any customer information at issue. The information security program developed should be flexible, designed to address the needs of the individual institution.

The final rules indicate that the objectives of the information security program should be

- to ensure the security and confidentiality of customer information;
- to protect against any anticipated threats to the security or integrity of such information; and

- to guard against the unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer.

Definitions. The rules include the following definitions for terms that appear in the regulations:

- *customer information* means any record containing nonpublic personal information[1] about a customer of a financial institution, whether in paper, electronic, or another form, that is handled or maintained by or on behalf of you or your affiliates.
- *information security program* means the administrative, technical, or physical safeguards you use to access, collect, distribute, process, protect, store, use, transmit, dispose of, or otherwise handle customer information.
- *service provider* means any person or entity that receives, maintains, processes, or otherwise is permitted access to customer information through its direct provision of services to a financial institution.

Required Elements of the Security Program. The rules set forth the elements that a financial institution is required to include in its information security program. The elements are intended to create a framework for developing, implementing, and maintaining the required safeguards. Institutions may tailor their programs, at their own discretion, to address their individual circumstances and needs.

The final rules require institutions to take the following steps in bringing about and maintaining their plans. Colleges and universities must

- designate an employee or employees to coordinate their information security program;
- identify reasonable, foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that could result in the unauthorized disclosure, misuse, alteration, destruction, or other compromise of such information, and assess the sufficiency of any safeguards in place to control these risks.
- at a minimum, such a risk assessment should include consideration of risks in each of the following operational areas:
  - employee training and management,
  - information systems, including network and software design, as well as information processing, storage, transmission, and disposal, and
  - detecting, preventing and responding to attacks, intrusions, or other systems failures;

design and implement information safeguards to control the risks identified through risk assessment and regularly test or monitor the effectiveness of the safeguards' key controls, systems, and procedures;

- oversee service providers by taking steps to select and retain providers that are capable of maintaining appropriate safeguards for customer information;
- contractually require their service providers by contract to implement and maintain such safeguards; and
- periodically evaluate and adjust their information security program, based on the results of the testing and monitoring mentioned above, any material changes to operations, or any other circumstances that are known to have or that may have a material impact on the information security program.

Effective Date

Institutions must implement an information security program no later than May 23, 2003. The rules allow for a grandfathering of service contracts entered into no later than June 24, 2002. FTC will extend the deadline to May 24, 2004, for a contract you have entered into with a third party to provide services or functions on behalf of your institution, even if the contract does not include a requirement that the service provider maintain appropriate safeguards.

Information Contacts

Additional guidance and compliance tips are available at www.ftc.gov/privacy/glbact. For questions related to the regulations, contact Laura D. Berger, Attorney, Division of Financial Practices at FTC, (202) 326-3224. The NACUBO contact, Mary M. Bachinger, senior policy analyst, may be reached by phone at (202) 861-2581 or by e-mail at mary.bachinger@nacubo.org.

1 16 CFR Part 313.3(n)(1) defines nonpublic personal information as "personally identifiable financial information; and any list, description, or other grouping of consumers (and publicly available information pertaining to them) that is derived using any personally identifiable financial information that is not publicly available." An example for colleges and universities would be information that a student provides on the Free Application for Federal Student Aid (FAFSA).