Safeguarding of Personal Financial Information by Higher Education Institutions

Under the Financial Services Modernization Act of 1999, also known as the Gramm-Leach-Bliley Act (GLBA), financial institutions have an affirmative and continuing obligation to respect the privacy of their customers and a duty to safeguard the security and confidentiality of their customers' nonpublic personal information. This legislation is enforced by the Federal Trade Commission (FTC), which has issued regulations specifying what steps financial institutions must take to comply with these privacy and safeguarding requirements.

The GLBA's definition of a "financial institution" is very broad. It includes any institution engaged in financial activities listed under the Bank Holding Company Act of 1956, including "making, acquiring, brokering, or servicing loans" and "collection agency services." As the FTC began the regulatory process, its proposed regulations were so expansive that higher education institutions feared their involvement in activities such as the making of Federal Perkins loans would qualify them as financial institutions under those regulations.

When the FTC sought comment on its proposed regulations for implementing the GLBA, the American Council on Education, the National Association of College and University Business Officers, and others asked the FTC to amend them to specifically exclude higher education institutions from those "financial institutions" subject to the GLBA. This request was based on the argument that it would not be consistent with congressional intent to interpret a law designed to modernize the financial services industry as imposing yet another layer of federal regulation and costs on higher education institutions. It was also pointed out that the Family Educational Rights and Privacy Act ("FERPA"), 20 U.S.C. § 1232g, has long provided ample privacy protection for student financial and other records maintained by higher education institutions.

In issuing its final regulations, the FTC concluded that higher education institutions are financial institutions subject to the GLBA. However, it agreed that these institutions would be deemed to be in compliance with the privacy rules of the GLBA regulations if they are in compliance with FERPA, and it amended the final regulations to so provide. Nonetheless, higher education institutions must comply with the administrative, technical, and physical safeguarding rules in the FTC regulations. The deadline for compliance with those rules is May 23, 2003.

The safeguarding rules require a written security plan that describes the institution's program to safeguard customer information. As a part of that plan, the institution must designate one or more employees to coordinate safeguards; identify and assess the risks to customer information in each relevant area of operations; evaluate the effectiveness of current safeguards; design and implement a safeguards program and regularly monitor and test it; select appropriate service providers and contract with them to implement safeguards; and evaluate and adjust the program in light of relevant circumstances, such as changing business arrangements or the results of testing and monitoring of safeguards.

The FTC regulations suggest that appropriate steps to safeguard customer information will include special care in the selection and training of employees who deal with that information, limitation of access to such information, and appropriate disciplinary action in cases of breach of confidentiality of such information. In addition, care must be taken to insure security of such information from data entry to data disposal. This will involve use of secure physical records storage areas and appropriate consideration of the security of electronic data storage and transmission, including the use of such measures as computer firewalls, strong password access controls, and detection/prevention of intrusion attempts. Finally, appropriate steps must be taken in the disposal of paper records as well as destructive erasure of data on tapes and hard drives.

Education institutions are being challenged to meet the increasing burden of the growing number of federal laws concerning privacy, each with its own set of regulatory requirements. The GLBA requirements summarized above join the long-standing requirements of FERPA, while the privacy requirements of the Health Insurance Portability and Accountability Act (HIPAA) are already in effect for most institutions and, in the case of small health plans, will become effective April 2004. Each of these laws is administered by a separate federal agency with no apparent effort by the various agencies to coordinate their implementing regulations, so as to avoid conflicting requirements or to agree upon a basic framework of requirements that would satisfy all three agencies. Nonetheless, compliance is essential, as failure to do so will jeopardize receipt of federal funding in the case of FERPA violations and may result in civil and criminal liability under GLBA and HIPAA.