



GLBA

The Office of Information Technology

Wednesday, April 06, 2005

Protecting secure data on our computer systems is a task of the utmost importance for which all of us must take responsibility...

Basically:

The security of our Student/Faculty/Staff (i.e. Customer) information is paramount. The GLBA Data Protection Rule and subsequent safeguards are mandated to:

1. Ensure the security and confidentiality of customer data.
2. Protect against any reasonably anticipated threats or hazards to the security or integrity of such data.
3. Protect against unauthorized access (including Computer Theft) to or use of such data that would result in substantial harm or inconvenience to any customer. (i.e. Students, Faculty and Staff).

A Little History:

On November 12, 1999, President Clinton signed the Gramm-Leach-Bliley Act (GLBA) into law. GLBA Section 501, Protection of Nonpublic Personal Information, requires federal banking agencies, the National Credit Union Administration, the Securities and Exchange Commission, and the Federal Trade Commission to establish appropriate standards for financial institutions related to the administrative, technical, and physical safeguards of customer records and information.

Notes following were drafted for the Educause 2003 Networking Conference:

<http://www.educause.edu/>

Information Security Programs Under Gramm-Leach-Bliley:

Q. What is the law?

A. The law is Financial Services Modernization Act of 1999[1][1], also known as the Gramm-Leach-Bliley Act (GLB). It regulates the disclosure of non-public personal information[2][2] by financial institutions. Institutions of higher education (IHEs) are covered by the law's definition of "financial institutions" as they participate in financial activities, such as offering Federal Perkins Loans.

Q. What does the law require of IHEs?

A. IHEs must have a written information security program. The purposes are threefold:

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

Q. Who is a customer?

A. A customer is defined as a consumer who has a customer relationship with you.[3][3] A consumer means an individual who obtains or has obtained a financial product or service from you that is used primarily for personal, family, or household purposes, or that individual's legal representative.[4][4] This would include a student who obtained a loan from the school or parents who sent in income tax information in connection with their child's application for a financial aid package.

However, as it does not make sense to have safeguards in place for only those students who have obtained loans from the university given practical issues as well as other laws such as FERPA, most IHEs will be considering a comprehensive security program. In the same vein, if you are protecting customer credit card information under the law, it makes sense to apply the security controls to all credit card information held by the IHE. The law covers both paper copies of information and electronic copies. The safeguarding provision applies not only to all such information about persons with whom the university has a customer relationship, but also pertains to customers of other financial institutions that have provided such information.

Q. What is customer information?

A. In a general sense, customer information typically gathered in connection with obtaining a financial product or service to includes names, addresses, phone numbers, bank and credit card account numbers, income and credit histories and Social Security numbers.[5][5]

Q. What is a financial product or service?

A. The term financial product or service is defined in 16 CFR 313.3(l)(1) as "any product or service that a financial holding company could offer by engaging in a financial activity under section 4(k) of the Bank Holding Company Act of 1956." That, in turn, takes you to certain sections of the Federal Reserve Board's so-called "Regulation Y," specifically 12 CFR 225.26 and 225.28. Regulation Y, which is permissive and therefore not a very apt vehicle for defining what GLB requires, includes the activities that we all agree are subject to GLB, like making student or faculty loans, as well as some oddities that may also be applicable to colleges and universities, like career counseling services to individuals who seek employment at financial institutions, and management consulting activities on any subject to a financial institution and on financial, economic, accounting, or audit matters to any company (which might apply to business school practicum programs).*

The FTC has agreed to work with the higher education community in defining how GLB applies to colleges and universities.

Q. What is the time frame?

A. The May 2002 regulations under this law dictate that by May 23, 2003 the IHE must have implemented an information security program. There are a number of components to the program, which will be addressed below. As long as the written plan is in place by May 23, 2003 (or a fairly comprehensive draft), it would seem the university would be exposed to minimal liability if the training is not completed by May 23, 2003, so long as implementation has begun.

Q. What are the general components of the program?

A. IHEs must develop, implement and maintain a comprehensive written information security program that contains administrative, technical and physical safeguards that are appropriate to the school's size and complexity, the nature and scope of the IHE's activities, and the sensitivity of any customer information at issue. The written program does not have to be all in one document, e.g. it can be a combination of policies, (perhaps some already in existence) that together equal a comprehensive policy. Review your existing policies and see where the gaps are.

Q. Didn't universities get an exemption from this law?

A. There are two different sets of rules under this law; the safeguarding rules at 16 CFR Part 314 and the privacy rules at 16 CFR Part 313. Institutions of higher education, while not exempt from the definition of "financial institutions," are generally excluded from the requirement to comply with the GLB privacy policy regulations as long as the institution complies with the Family Educational Rights and Privacy Act. IHEs are not exempt from the safeguards requirements of the law. The final rules on the safeguarding program came out in May 2002.

* This answer on financial product or service provided courtesy of Jeff Swope, Palmer and Dodge, LLP