Connecticut State University System

Developing a State of Minds

RESOLUTION

concerning

GRAMM-LEACH-BLILEY ACT COMPLIANCE

January 27, 2006

WHEREAS, Federal Trade Commission (FTC) rules implementing the Gramm-Leach-Bliley Act, 15 U.S.C. § 6801, et seq. (GLBA) require that financial institutions 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 the customer information or data at issue, and

WHEREAS, Because higher education institutions participate in financial activities, such as making Federal Perkins Loans, FTC regulations consider them financial institutions for GLBA purposes, and

WHEREAS, Information security as referred to in GLBA pertains not only to securing of electronic information, devices, and media but also to paper files and physical locations, and

WHEREAS, The FTC rules set forth the elements that a financial institution is required to include in its information security program, which are intended to create a framework for developing, implementing, and maintaining the required safeguards, and

WHEREAS, Institutions may tailor their programs, at their own discretion, to address their individual circumstances and needs, and

WHEREAS, The rules required that all institutions initially develop and implement a written GLBA information security program no later than May 23, 2003, and

WHEREAS, GLBA information security programs were initially implemented by each university and the System Office prior to the implementation of the CSU Systemwide Information Security Policy, therefore be it

RESOLVED, That each university and the System Office shall maintain a Gramm-Leach-Bliley Act (GLBA) compliance policy conforming to the safeguarding requirements of the GLBA (16 CFR Part 314) and other applicable statutes and regulations, and consistent with the CSU Systemwide Information Security Policy, and be it further

RESOLVED, That each university and the System Office shall review and update its GLBA compliance policy as conditions warrant, but not less than every three years; with the first review and any necessary revisions to be completed by June 30, 2006, and be it further

RESOLVED, That each university and the System Office shall conduct training annually for all appropriate employees regarding GLBA compliance, and be it further

RESOLVED, That each university and the System Office shall annually provide to the Board of Trustees a report detailing the GLBA training provided at their location.

A Certified True Copy:

Lawrence D. McHugh
Chairman

ITEM

Gramm-Leach-Bliley Act compliance

BACKGROUND

Federal Trade Commission (FTC) regulations set forth at 16 CFR Part 314, published in May 2002 (May 23 *Federal Register*, p. 346484) were promulgated under the Gramm-Leach-Bliley Act (GLBA), 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.

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

ANALYSIS

The GLBA 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 GLBA purposes.

The FTC promulgated two sets of rules to implement the GLBA: the privacy rules (16 CFR Part 313, and the safeguarding rules (16 CFR Part 314). Colleges and universities are deemed to be in compliance with the FTC's privacy rules if they are in compliance with the Family Educational Rights and Privacy Act (FERPA). However, higher education institutions are subject to the FTC's rules relating to the administrative, technical, and physical safeguarding of customer information.

Financial institutions, including colleges and universities, must "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. FTC 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. It is important to note that information security as referred to in GLBA refers not just to electronic information, media (diskettes, CD's, etc.), and devices (such as PDA's and laptops), but also to paper files and the securing of the physical locations where these files are stored.

The FTC safeguarding rules required that all institutions develop and implement a written GLBA information security program no later than May 23, 2003, which was prior to the implementation of

the CSU Systemwide Information Security Policy. However, it is important that the existing GLBA compliance policies in effect at the various CSU universities and the System Office be consistent with the CSU Systemwide Information Security Policy, and that they be reviewed regularly to ensure continuing relevance as conditions change. This resolution would require that the GLBA compliance policies in effect at the CSU universities and the System Office not only conform to all applicable statutes and regulations, but also are consistent with the CSU Systemwide Information Security Policy. It would further require that the GLBA compliance policies be reviewed (and revised as necessary) at least every three years, with the first review to be completed by June 30, 2006, and that all appropriate CSU employees receive GLBA compliance training on an annual basis, to ensure an awareness and understanding of the importance of information security and compliance with the policy. Finally, it would require an annual report to the Board of Trustees by each university and the System Office regarding GLBA training provided.

CHANCELLOR'S RECOMMENDATION

That each university and the System Office maintain a Gramm-Leach Bliley Act compliance policy conforming to the safeguarding requirements of the GLBA (16 CFR Part 314) and other applicable statutes and regulations, and consistent with the CSU Systemwide Information Security Policy; that each university and the System Office review and update its GLBA Compliance Policy as conditions warrant, but not less than every three years, with the first review and any necessary revisions to be completed by June 30, 2006; that each university and the System Office conduct annual training sessions for all appropriate employees regarding GLBA compliance; and that each university and the System Office provide the Board of Trustees with an annual report detailing the GLBA training provided at their respective locations.