NAIS LEGAL ADVISORY

THE GRAMM-LEACH-BLILEY ACT FOR INDEPENDENT SCHOOLS

Timothy Tobin, Partner
Michael Epshteyn, Associate
Of Hogan Lovells US LLP
February 2014

Introduction

The federal Gramm-Leach-Bliley Act ("GLBA")[1] regulates the privacy and security of personal financial information, referred to as nonpublic personal information. GLBA applies to "financial institutions," a term that is defined very broadly and encompasses not only banks but also any entity that is "significantly engaged" in certain financial activities. Although schools are not considered financial institutions in the traditional sense, they may be considered financial institutions under this law to the extent that they conduct financial activities such as lending or providing financial advisory services. For example, a school that issues loans to students or staff, or provides financial counseling to donors, may be considered a financial institution under GLBA if it is "significantly engaged" in such activities.[2] Whether a school is "significantly engaged" in these activities involves a fairly fact-specific analysis. In higher education, where the institutions regularly engage in such activities, the answer is clearer. However, for many schools at the K-12 level, the assessment will depend on each school's activities. If your school is a larger school that tends to have more complex activities in both loans and donor or employee advising with regard to financial advising, it may be that providing some of the requirements under the GLBA is in your school's best interest.

[1] Gramm-Leach-Bliley Financial Modernization Act of 1999, Pub. L. 106-102, 113 Stat. 1338 (codified as amended at scattered sections of 12 U.S.C.,15 U.S.C., 18 U.S.C., and 29 U.S.C.).

[2] The phrase "significantly engaged" is not defined; however, regulatory guidance suggests that an entity that conducts a financial activity on a regular basis is significantly engaged in the activity for purposes of GLBA, even if that activity does not constitute the majority of its business.

Regulations under the GLBA

Five federal banking agencies, the Securities and Exchange Commission ("SEC"), and the Federal Trade Commission ("FTC") have issued rules and guidelines implementing the privacy and security provisions of GLBA. Non-banking financial institutions and entities that are not broker-dealers or SEC-regulated investment advisors, such as schools, are regulated under the FTC's GLBA regulations (known as the "Privacy Rule" and the "Safeguards Rule"). The Privacy Rule addresses financial institutions' permissible uses and sharing of personal financial information and the Safeguards Rule addresses reasonable protections for such information.

Notably, the FTC's Privacy Rule provides that an "institution of higher education" that complies with the Federal Educational Rights and Privacy Act ("FERPA") and its implementing regulations will also be deemed in compliance with the Privacy Rule.[3] Although FERPA applies not only to institutions of "higher education," but also to elementary and secondary schools that receive funds under a U.S. Department of Education-administered program,[4] the Privacy Rule exception for FERPA-regulated entities as written is limited to institutions of higher education. Therefore, a K-12 school that qualifies as a financial institution under GLBA may be subject to the Privacy Rule, even if it is also covered by and in compliance with FERPA.

Additionally, unlike the Privacy Rule, the FTC's Safeguards Rule does *not* include an exception for FERPA-regulated institutions of higher education. Accordingly, schools that meet the definition of a "financial institution" may be subject to GLBA's privacy and security requirements. An overview of those requirements is provided below.

Privacy Rule

As the name might suggest, the Privacy Rule requires entities regulated as financial institutions to give privacy notices to their customers and, subject to certain exceptions, gives customers and consumers the right to limit the financial institution's sharing of their "nonpublic personal information" with nonaffiliated third parties, if such sharing might occur.

This nonpublic personal information includes any information:

---

[3] 16 C.F.R. § 313.1.

[4] FERPA applies to educational agencies or institutions (including primary/secondary and postsecondary education institutions) to which funds have been made available under a U.S. Department of Education-administered program. *See* 20 U.S.C. 1232g; 34 C.F.R. § 99.1. For more information on this topic, see *Top Federal Programs: Are They Triggering Obligations for Your School?* on *www.nais.org*.

(i) that a consumer provides to obtain a financial product or service (such as information submitted in an application);

(ii) about a consumer resulting from a transaction between the consumer and the institution; and

(iii) that a financial institution otherwise obtains about a consumer (such as credit report information).[5]

The term "customer" means a consumer who has a continuing relationship with the financial institution.[6] A "consumer" is an individual who obtains a financial product or service primarily for personal, family, or household purposes.[7] Although schools may not typically consider themselves to have "customers" or "consumers," in the context of the Privacy and Safeguards Rules, if deemed to be a financial institution, any personal data obtained by a school while providing a financial service (such as making loans) would be nonpublic personal information.

Under this rule, the school must give each customer an "initial notice," at the time the customer relationship is established. The notice describes how the institution collects, discloses, and protects nonpublic personal information.[8] Also, the institution must give each customer an "annual notice" of its privacy practices for as long as the customer relationship lasts.[9] If the institution shares nonpublic personal information with unaffiliated third parties (and the sharing does not fall within certain exceptions), the institution must provide customers and consumers with an "opt out notice" that clearly and conspicuously describes their right to opt out of the sharing of the information.[10] The Privacy Rule sets forth the required elements of these notices, and the FTC, SEC, and federal banking agencies have issued a model privacy form that can be relied upon to satisfy the notice requirements.[11]

There are a number of exceptions to the opt-out requirement, including the sharing of information with service providers.[12] Under this exception, a consumer does not have the right

[5] *Id*. § 313.3(n) & (o).
[6] *Id*. § 313.3(h).
[7] *Id*. § 313.3(e)(1).
[8] *Id*. § 313.4.
[9] *Id*. § 313.5.
[10] *Id*. § 313.7.
[11] The model privacy form is available at http://www.ftc.gov/privacy/privacyinitiatives/PrivacyModelForm.pdf. Although use of the model form is not mandatory, a financial institution that chooses to use the model privacy form consistent with the instructions to the form will be guaranteed to satisfy the disclosure requirements for privacy notices under GLBA (i.e., will obtain a "safe harbor").
[12] *Id*. § 313.13.

to limit a financial institution's sharing of information with a nonaffiliated third party that performs services or functions on behalf of the financial institution, such as marketing the financial institution's own products or services. However, the financial institution must enter into a contract with the service provider that prevents it from disclosing the information or using the information other than to carry out the purposes for which it was disclosed by the financial institution.[13]

Safeguards Rule

The second major rule that regulated schools have to comply with is the Safeguards Rule. Under the Safeguards Rule, each institution is required to implement a written information security program that includes administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of "customer information."[14] Customer information is defined as nonpublic personal information about a customer of a financial institution, whether in paper, electronic, or other form.[15]

As part of its information security program, a financial institution must:

- designate an employee to coordinate its program;
- identify and assess the risks to customer information in each relevant area of the institution's operation, and evaluate the effectiveness of the current safeguards for controlling these risks;
- design and implement a safeguards program, and regularly monitor and test it;
- evaluate and adjust the program in light of relevant circumstances, including changes in the institution's business or operations, or the results of security testing and monitoring;
- oversee service providers,[16] including requiring them by contract to implement and maintain appropriate safeguards; and
- evaluate and adjust the safeguards program in light of the results of regular testing and monitoring, any material changes to the institutions operations or business arrangements, or any other circumstances that may have a material impact on the institution's information security program.[17]

[13] *Id*. § 313.13(a)(1)(ii).
[14] 16 C.F.R. § 314.3.
[15] *Id*. § 314.2(b).
[16] The term "service provider" is defined broadly and includes any person or entity that maintains, processes, or otherwise is permitted access to customer information through the provision of services directly to the financial institution. *Id*. § 314.2(d).
[17] *Id*. § 314.4.

The Safeguards Rule does not require a "one size fits all" solution for institutions' information security programs; rather, each institution must develop a program that is "appropriate" to its size and complexity, the nature and scope of its activities, and the sensitivity of the customer information at issue.[18] Therefore, a school may exercise some latitude in developing its GLBA information security program. Moreover, a school can incorporate the administrative, physical, and technical safeguards required under the Safeguards Rule, as appropriate, into its existing data security policies and procedures, such as its acceptable use policy, IT security policy, and policies governing access to student records.

In short, when implementing these requirements, a school should assign an individual to oversee the data safeguarding, review the data that it collects, review how the information is currently safeguarded, and make adjustments as needed to ensure that the information is safe. The final safeguards should be in place within the policies, procedures, and technological measures and regularly reviewed to ensure they are still appropriate. Schools that use vendors should include provisions within their contracts requiring vendors to also comply with the safeguard rules.

Payment Plans

A potentially common triggering compliance factor for schools is the extension of payment plans to families. While conclusive guidance from the FTC in this area is difficult to come by, FTC meeting notes and informal guidance to the Coalition of Higher Education Assistance Organizations (COHEAO) and FTC officials in 2003 notes that payment plans that charge interest likely trigger the GLBA privacy rule requirements.[19] Other than this informal guidance, the FTC has not offered any other clarifications on this topic. Schools that do offer installment agreements for tuition that charge interest should be aware of the potential obligations under the GLBA.

---

[18] *Id*. § 314.4(a).

[19] *See* http://www.nacubo.org/documents/business_topics/COHEAO_notes.doc), FTC attorneys "pointed to the preamble of the regulations and said that extension of credit meets that criterion [for a financial transaction], while installment contracts probably do not. Payment of tuition and fees in more than one installment is not considered an extension of credit, unless the installment contract is in the form of a loan that charges interest." (emphasis added)

Conclusion

Schools that have not yet evaluated whether they are engaged in activities that make them a "financial institution" under GLBA should conduct that assessment. Schools that previously concluded that they are not financial institutions should consider whether they have undergone any changes in their operations or activities that would affect their status under GLBA. Covered schools should take appropriate steps to comply with the Privacy Rule and to implement and maintain a written information security in accordance with the Safeguards Rule—both to facilitate regulatory compliance and, no less importantly, to help ensure that they are serving as responsible stewards of their students', faculty members', and other individuals' sensitive personal information.