October 31, 2018

Gramm-Leach-Bliley Act - Are you protecting your students' financial data?

AUDIT, HIGHER EDUCATION, NOT-FOR-PROFIT
BY MICHAEL WITHROW

The Gramm-Leach-Bliley Act (GLBA) is a federal law that applies to entities that collect consumer financial data, including institutions of higher education. This law, specifically the Safeguards Rule, applies to how higher education institutions collect, store, and use student financial records containing personally identifiable information (PII). Some examples of student data that need to be protected under the GLBA include information provided on the Free Application for Federal Student Aid (FAFSA), student application information, and student information shared with loan servicers. Higher education institutions have been required to comply with the provisions of the GLBA since 2003; however, there has not been much enforcement by the Department of Education (DOE) related to the GLBA. This is about to change.

The U.S. Office of Management and Budget announced that it plans to add new Special Tests and Provisions to its 2019 *Compliance Supplement*, with the DOE including the testing requirements in the *Audit Guide* shortly thereafter. As a result, higher education institutions' compliance with the GLBA will most likely be tested as part of your institution's Single Audit starting in 2019. The DOE has cautioned higher education institutions that data security and student privacy are becoming critical issues. Failure to comply with GLBA provisions may bring penalties that range from monetary fines to the restriction or loss of eligibility for certain federal funding.

So, what does your institution need to do in order to ensure compliance with the GLBA and prepare for upcoming Single Audits? The Safeguards Rule requires institutions to develop, implement, and maintain a written information security program that includes the following components:

- Designate an information security officer for coordinating the information security program.
- Assess the risks to confidential information, assess the level of controls in place, and identify action plans to address the risks.
- Implement an information security program, including various technical and physical underlying controls.
- Oversee vendor relationships to ensure confidential data is secured at their locations when applicable and access is controlled when vendors utilize PII from the institution.
- Perform an ongoing evaluation of the program to keep content current with the changing security environment.

In addition to developing a program, institutions must properly train employees, managers, staff, and their vendors on their data security protocols and ensure there is ongoing training and monitoring. The employees responsible for implementation and management of the program must understand it, recognize its importance, and be incentivized to follow and adhere to it. Management must ensure that violations of the program are addressed appropriately. Vendors that aren't able to comply with the necessary safeguards must be replaced.

How will this change impact your audit? External auditors will be required to conduct expanded audit testing and report significant noncompliance findings if the institution has complied with these requirements. This will add another layer of complexity and effort to the audit process. The DOE suggested the following audit procedures be tested as part of the auditors' compliance audit:

- Verify that an institution has designated an individual to coordinate the information security program.
- Obtain the institution's risk assessment and verify that it addresses the required standards for safeguarding customer information.
- Obtain documentation of the institution's safeguard that aligns with each risk identified from the risk assessment and verify that the institution has identified a safeguard for each risk.

These rules will be finalized as part of the vet copy of the Compliance Supplement, which will be released in the spring of 2019.

For additional information, please refer to the following resources:

https://www.ftc.gov/tips-advice/business-center/guidance/financial-institutions-customer-information-complying

https://www.gao.gov/products/GAO-18-121

You've heard our thoughts… We'd like to hear yours

The Schneider Downs Our Thoughts On blog exists to create a dialogue on issues that are important to organizations and individuals. While we enjoy sharing our ideas and insights, we're especially interested in what you may have to say. If you have a question or a comment about this article – or any article from the Our Thoughts On blog – we hope you'll share it with us. After all, a dialogue is an exchange of ideas, and we'd like to hear from you. Email us at contactSD@schneiderdowns.com.