STRADLEY RONON

Client Alert

A Publication of Stradley Ronon's
Cyber and Education Practice Groups

WWW.STRADLEY.COM

FEBRUARY 6, 2019

Stradley Ronon Stevens & Young, LLP
2005 Market Street
Suite 2600
Philadelphia, PA 19103-7018
215.564.8000 Telephone
215.564.8120 Facsimile
www.stradley.com

With other offices in:
Washington, D.C.
New York
New Jersey
Illinois
Delaware

Compliant Cybersecurity Protocols: A Prerequisite for Title IV Eligibility

by Kristin J. Jones and Mischa S. Wheat

By the second quarter of 2017, the federal government projected that there were over 42 million borrowers across all federal student loan programs. As the front-line administrators of many of these programs, higher education institutions have to collect and store a substantial amount of sensitive personal and financial data. Higher education institutions have a legal obligation to safeguard this data with information security controls derived from the same federal regulations applicable to sophisticated lending and banking institutions. The Department of Education has exercised little oversight to ensure that colleges and universities have compliant cybersecurity measures in place. In 2019, that is likely to change.

The Gramm-Leach-Bliley Act (GLBA) – more well-known in the world of finance and insurance than in education – created a source of federal regulatory authority that treats educational institutions as akin to financial institutions. Since GLBA was signed into law, federal regulatory agencies – such as the Federal Trade Commission – have promulgated new rules regarding the protection and storage of consumer financial information. These rules imposed affirmative responsibilities on "financial institutions" to implement sufficient protocols to safeguard customers' sensitive data. Because a significant amount of lending activity flows through colleges and universities, those institutions are considered "financial institutions" subject to the same regulatory framework, even though educational institutions were not GLBA's regulatory focus at its inception. Failure to comply with these regulations, however, can cause a post-secondary institution to suffer significant penalties, including loss of eligibility for Title IV funding.

To be in compliance with GLBA, a college or university must do the following:

- Conduct a risk assessment addressing employee training and management, the structure of information systems (including network and software design, as well as information processing, storage, transmission and disposal), and detection, prevention and response to attacks, intrusions or other system failures.
- Identify reasonably foreseeable internal and external risks to information security, confidentiality and integrity, and implement safeguards to control identified risks.
- Regularly test or monitor the effectiveness of the safeguards' key controls, systems and procedures.
- Oversee vendors by selecting and retaining service providers that have appropriate safeguards, and contractually requiring service providers to implement and maintain safeguards.
- Designate a person or team to coordinate its information security program.

- Evaluate and adjust the institution's information security programs in response to any new material conditions that affect security.

Colleges and universities have been required to comply with these cybersecurity regulations since they became effective in 2003, but compliance has yet to be subject to regular oversight. In the subsequent years, however, multiple news cycles have been dominated by high-profile data breaches that have created an ever-growing public concern about data security and recognition of an expanding cyberthreat. As a result, the Department of Education has indicated its intention in the near future to make GLBA compliance a part of the annual audit it requires on Title IV funds.

In 2019, educational institutions should be prepared to demonstrate their compliance with GLBA. In advance of this year's audit, colleges and universities should re-examine their documented threat response plans and consult with internal information security personnel. The risks to personal and financial data have become more complicated and expansive since 2003, and to demonstrate GLBA compliance, an educational institution's cybersecurity stance should respond in kind.

Kristin J. Jones, CIPP/US

Mischa S. Wheat

For more information, contact Kristin J. Jones at 484.323.1355 or kjones@stradley.com or Mischa S. Wheat at 215.564.8597 or mwheat@stradley.com.