

### New York State Department of Financial Services to Implement Regulations Applicable to All Entities Regulated under the Insurance Law, including some Colleges, Universities, and Charitable and Religious Organizations

Following a public comment period, the New York State Department of Financial Services (DFS) has published a modified version of new regulations, previously issued on September 13, 2016, aimed at creating higher cybersecurity standards within the banking, insurance and financial services industries. The regulations go into effect on March 1, 2017 with phased implementation thereafter, and will likely require significant capital expenditures and operational changes by colleges, universities and charitable and religious organizations covered by the regulations. The public comment period for the proposed modified regulations will be open until January 27, 2017.

Colleges and universities must already comply with a panoply of laws, regulations and standards relating to data security: the Gramm-Leach-Bliley Act, the United States Department of Education guidance applicable to student loan information, the Red Flags Rule, PCI standards for credit card information, and, for some institutions, the Health Insurance Portability and Accountability Act. Charitable and religious corporations may also be bound by these standards, depending on their programs and operations. The DFS proposed cybersecurity regulations would impose operational requirements and expenditures that are far more burdensome than the regulatory obligations already mandated for institutions of higher education and charitable and religious organizations in many respects, including but not limited to standards for: penetration testing and vulnerability assessments, audit trails, cybersecurity personnel, due diligence, risk assessment, and contracting with third parties, use of multi-factor authentication and annual certification of compliance by the board of directors.

For information on the specific requirements of the proposed cybersecurity regulations, please review our Client Information Memoranda dated [September 16, 2016](#) and [January 6, 2017](#). The complete text of the proposed regulations, which go into effect on March 1, 2017, can be found [here](#). Set forth below is an analysis of which entities are covered by or exempt from the proposed regulations.

**Covered Entities.** The new cybersecurity regulations apply to “Covered Entities”, which are defined broadly as “any Person operating under or required to operate under a license, registration, charter, certificate, permit, accreditation or similar authorization under the banking law, the insurance law or the financial services law.” Among the 3,800 entities regulated by DFS is a subset of institutions and organizations that are engaged in bona fide charitable, religious, missionary, educational or philanthropic activities and are permitted under N.Y. Insurance Law § 1110 to issue charitable gift annuities to donors. Therefore, unless the new regulations are further modified, such entities (including many colleges, universities, and religious and charitable organizations) will be required to comply. To determine if your entity is supervised by DFS, you can perform a search [here](#).

It is not immediately clear that DFS intended to include entities regulated solely under Insurance Law § 1110 as covered entities alongside traditional insurance companies. In fact, according to the Report on Cyber Security in the Insurance Sector, which was conducted as part of the regulation drafting process, DFS surveyed 21 health insurers, 12 property and casualty insurance providers, and 10 life insurance providers, but no colleges, universities, or charitable or religious organizations. Statements made by the Superintendent of Department of Financial Services, Maria T. Vullo, and Governor Andrew Cuomo in connection with the announcement of the regulations make no mention of not-for-profit organizations or higher education institutions as targets of the regulations.

Notwithstanding the apparent primary focus of the regulations, in connection with its reissuance of the regulations on December 28, DFS acknowledged that many of the comments it received concerned the broad definition of “Covered Entity”, but that it opted not to amend that definition at this time. Organizations and institutions may wish to submit public comments about the impact of the regulations on their organizations during the current public comment period, but should proceed on the assumption that the regulations will apply unless and until DFS provides definitive guidance to the contrary.

**Exempt Entities.** Certain covered entities are exempt from a subset of the new cybersecurity regulations. Exempt entities include those with fewer than 10 employees, less than \$5 million gross annual revenue for three year, or less than \$10 million in year-end total assets. Additional exemptions exist for covered entities that do not operate, maintain, utilize or control any Information Systems and do not control, own, access, generate, receive or possess Nonpublic Information as those terms are defined by the regulations. Covered entities that qualify for exemptions must file a “Notice of Exemption” with DFS affirming the basis for the exemption.

If you have any questions about this Information Memorandum, please contact [Philip J. Zaccheo](#), [Tracy E. Miller](#) or [Curtis A. Johnson](#) or the attorney in the firm’s Cybersecurity and Data Privacy Practice, Higher Education Practice, or Exempt Organizations Practice with whom you are regularly in contact.



Commitment • Service • Value • Our Bond



Bond, Schoeneck & King PLLC (Bond, we, or us), has prepared this communication to present only general information. This is not intended as legal advice, nor should you consider it as such. You should not act, or decline to act, based upon the contents. While we try to make sure that the information is complete and accurate, laws can change quickly. You should always formally engage a lawyer of your choosing before taking actions which have legal consequences. For information about our firm, practice areas and attorneys, visit our website, [www.bsk.com](http://www.bsk.com). • Attorney Advertising • © 2017 Bond, Schoeneck & King, PLLC, One Lincoln Center, Syracuse, NY 13202 • 315.218.8000.

CONNECT WITH US ON LINKEDIN: SEARCH FOR BOND, SCHOENECK & KING, PLLC

FOLLOW US ON TWITTER: SEARCH FOR BONDLAWFIRM