BOND SCHOENECK & KING

600 Third Avenue, 22nd Floor | New York, NY 10016-1915 | bsk.com

TRACY E. MILLER
tmiller@bsk.com
P: 646.253.2308
F: 646.253.2364

January 27, 2017

VIA ELECTRONIC MAIL CyberRegComments@dfs.ny.gov

Cassandra Lentchner
Deputy Superintendent for Compliance
New York State Department of Financial Services
One State Street
New York, NY 10004

Re: Proposed Cybersecurity Requirements for Financial Services Companies

Dear Ms. Lentchner:

We are writing to provide comments on the revised, proposed cybersecurity regulations, 23 NYCRR § 500.01 et. seq. ("Revised Regulations") promulgated by the New York State Department of Financial Services ("DFS"). We are joined in these comments by the Commission on Independent Colleges and Universities ("CICU").

Many of the hundreds of colleges and universities and not-for-profit organizations that will be governed by the Revised Regulations ("Covered Entities") are Covered Entities due to the fact that they have a permit pursuant to N.Y. Insurance Law § 1110 to issue charitable gift annuities to donors. The regulations as initially proposed, and as amended, do not appear to have been designed for institutions of higher education and not-for-profit organizations, and are ill-suited to those organizations. In contrast to banks and other financial institutions that engage in financial transactions as the core of their operations, providing an annuity program for donors is tangential to the mission of colleges, universities, and not-for-profit organizations, and is not a sound basis to bind these organizations to regulations developed principally for financial institutions. For the reasons set forth below, the Revised Regulations should be amended to exempt organizations deemed a Covered Entity solely on this basis.

Pursuant to N.Y. Insurance Law § 1110, organizations that operate an annuity program for donors must have a permit from DFS. For many institutions of higher education and not-for-profit organizations, this permit is the sole basis for their status as a Covered Entity under the Revised Regulations. Yet, under the broad definitions of "information systems" and "nonpublic information (NPI)" set forth in the Revised Regulations, all categories and types of confidential information maintained by colleges, universities, and not-for-profit organizations will be swept into the ambit of the Revised Regulations. This will impose a costly, onerous regulatory scheme and obligations on institutions already bound by other cybersecurity laws and standards.

As large, complex institutions, colleges and universities hold many kinds of NPI, including student data, employee data, research data, intellectual property and health clinic information. The Revised Regulations would be a regulatory overlay for all data held by institutions that are already highly regulated in relation to cybersecurity practices. Colleges and universities must comply with four distinct sets of federal regulations and standards for cybersecurity: the Family Educational Rights and Privacy Act, the Gramm-Leach-Bliley Act, the Red Flags Rule, and, for the many colleges and universities that operate health care clinics that serve faculty, staff or individuals other than students, the Health Insurance Portability and Accountability Act ("HIPAA") and the implementing regulations of the HIPAA Security Rule. In addition, as entities that rely upon credit cards for student use, colleges and universities must satisfy the Payment Card Industry Data Security Standard.

Other not-for-profit organizations covered by the Revised Regulations based on holding a permit for an annuity program range from museums and other cultural institutions to social service organizations, religiously-affiliated service organizations, and advocacy organizations. They vary widely in size, budget, data maintained, and mission. For small not-for-profit entities, the Revised Regulations will impose an onerous financial and administrative burden unrelated to the size, resources, or the sensitivity of information they maintain and their operations. Not-for-profit organizations that provide health care services are already bound by the HIPAA Security Rule which mandates robust obligations to protect the security of medical records.

In many cases, institutions of higher education and not-for-profit organizations rely on banks to manage their donor annuity programs, which serve as the repository for NPI about donors. In these instances, NPI for annuity programs is fully protected by organizations bound to comply with the Revised Regulations. Imposing the Revised Regulations on colleges and universities and not-for-profit organizations in these many cases is therefore redundant to protect the NPI in donor annuity programs, and yet would encompass the information systems and other NPI held by these organizations to carry out the many activities integral to their mission.

For the reasons stated above, we urge that the Revised Regulations be amended to create an exemption for organizations that are bound by the Revised Regulations solely because they hold a permit for a donor annuity program. If this recommendation is not accepted, we request that an exemption be provided for organizations covered by the Revised Regulations solely because they have a permit for an annuity program, if they submit a request for exemption to DFS, stating that they do not maintain, use, or have access to NPI through the donor annuity program, and that another Covered Entity maintains and manages that data on the organization's behalf.

We appreciate the opportunity to offer these public comments.

Very truly yours,

BOND, SCHOENECK & KING, PLLC

Tracy E. Miller

TEM/dd