CONSUMER DATA INDUSTRY ASSOCIATION
Empowering Economic Opportunity
Writer's Direct Dial: 202.408.7407
Writer's email: eellman@cdiaonline.org

January 25, 2017

Via Electronic Delivery

Ms. Cassandra Lentchner
Deputy Superintendent for Compliance
New York State Department of Financial Services
One State Street
New York, NY 10004-1511

Via email: CyberRegComments@dfs.ny.gov

RE: Comments in Response to Proposed Rule 23NYCRR500 Cybersecurity Requirements for Financial Services Companies.

Dear Ms. Lentchner:

I write on behalf of the Consumer Data Industry Association ("CDIA") to submit a comment on revised cybersecurity rule issued by the Department of Financial Services ("DFS"). We greatly the changes made between the initial rule and the most recent rule. Our comment now, in follow-up to our earlier comment, focuses on a further change we would like to see in 500.11(b)(2) to clarify confusion caused by the rule.

CDIA is an international trade association, founded in 1906, of more than 130 corporate members. Its mission is to enable consumers, media, legislators and regulators to understand the benefits of the responsible use of consumer data which creates opportunities for consumers and the economy. CDIA members provide businesses with the data and analytical tools necessary to manage risk. They help ensure fair and safe transactions for consumers, facilitate competition and expand consumers' access to a market which is innovative and focused on their needs. CDIA member products are used in more than nine billion transactions each year.

CDIA members are primarily third parties under the revised rule and we remain concerned that unduly harsh provisions for covered entities will have more unnecessary burdens on third-party service providers. For this reason, we remain concerned with the encryption requirement for third-party servicers. Under Section 500.11(b)(2), third-party service providers would have an obligation to encrypt data both in transit and at rest. However, under Sec. 500.15, a covered entity must "implement controls, including encryption" – implying that encryption is not mandated for such entities. To clarify the likely confusion, Sec. 500.11(b)(2) should be rewritten to not mandate a specific technology. We respectfully suggest that Sec. 500.11(b)(2) be revised as follows:

> (2) the Third Party Service Provider's policies and procedures to implement controls, including the use of encryption, ~~as defined by section 500.15~~ to protect Nonpublic Information in transit and at rest;

We hope that this information is helpful to you. We feel that such changes to Sec. 500.11(b)(2) will clarify confusion that might be caused by the regulation.

Respectfully submitted,

Eric J. Ellman
Interim President & Chief Executive Officer
Senior Vice President, Public Policy & Legal Affairs