NEW YORK'S PROPOSED CYBERSECURITY REQUIREMENTS FOR FINANCIAL SERVICES COMPANIES – RIPPLE EFFECT ACROSS THE FINANCIAL SERVICES INDUSTRY

BY ALAN S. WERNICK, ESQ.

When speaking with executives in the C-Suite or directors of the boards of financial services companies, one concern shared by most of them is cyber threats. Whether it is their concern about not really understanding the risks, the financial losses, remediation expenses, reputational damages, or potentially the loss of their job, there's a simmering awareness that cyber threats are no longer just a problem for the IT department. While there already exists a number of laws and regulations dealing with cyber threats and data breaches that affect banks, insurance companies, other financial services companies, and other businesses, government regulators are continuing to examine and propose new regulations to address these threats.

One recently proposed regulation aimed at cyber threats against financial services companies is the New York Department of Financial Services ("DFS") proposed "Cybersecurity Requirements For Financial Services Companies" ("CRFSC") (23 NYCRR 500) which is scheduled to become effective on January 1, 2017 (subject to a 180-day transitional period to allow Covered Entities to comply). Although these cybersecurity requirements are focused at financial services companies under the jurisdiction of DFS, the reach of these regulations may affect companies outside of New York who are doing business with financial services companies in New York and may serve as a model for other financial service regulators.

As New York Governor Cuomo said in a September 13, 2016, press release announcing the DFS proposed regulations: "This regulation helps guarantee the financial services industry upholds its obligation to protect consumers and ensure that its systems are sufficiently constructed to prevent cyber-attacks to the fullest extent possible."

The DFS (like other government regulatory agencies) has enforcement authority to impose fines and penalties for violations of its regulations, as well as ordering licensing suspensions, policies and procedures reformation, and mandated separation or termination of high level employees of financial services companies.

Who is subject to 23 NYCRR 500?

The NY DFS 23 NYCRR 500 regulation for cybersecurity requirements for financial services companies provides several detailed definitions concerning who is subject to the regulation. Suffice it to say if you are a bank, insurance company, or other financial services company subject to New York's DFS licensing and regulations, or doing business as a third party service provider with a bank, insurance company or other financial services company in New York, or if you receive any "Nonpublic Information" (which is broadly defined in the regulation) from a "Covered Entity" (as defined in the regulations), then you may be subject, in whole or in part, to this DFS 23 NYCRR 500 regulation.

What are some of the 23 NYCRR 500 compliance requirements?

The NY DFS 23 NYCRR 500 regulation proposes several compliance requirements on Covered Entities and certain third parties doing business with Covered Entities including:

1. Creating and maintaining a written cybersecurity program designed to ensure the confidentiality, integrity, and availability of the Covered Entity's Information Systems, and designed to perform several core cybersecurity functions identified in 23 NYCRR 500.
2. Creating, implementing, and maintaining a written cybersecurity policy. The cybersecurity policy must be reviewed by the Covered Entity's board of directors ("BOD" – or equivalent governing body), and approved by a Senior Officer of the Covered Entity (and if no such BOD or equivalent governing body exists, then the cybersecurity policy must be reviewed and approved by a Senior Officer of the Covered Entity). The 23 NYCRR 500 DFS regulation suggests certain minimum criteria the cybersecurity policy should address.
3. Designating a qualified individual to serve as the Covered Entity's Chief Information Security Officer ("CISO") responsible for overseeing and implementing the Covered Entity's cybersecurity program and enforcing its cybersecurity policy. If the Covered Entity wants to meet this requirement using third party service providers, then the Covered Entity must, nonetheless, retain responsibility for compliance with these cybersecurity regulations, and identify a senior member of the Covered Entity who has oversight over the third-party service provider. Also, in addition to the Covered Entity retaining

responsibility for compliance with these regulations, the third-party service provider must also adhere to these regulations. This means that the contracts between these parties must be carefully drafted to properly allocate the risks of non-compliance with the requirements of the DFS regulations.

4. Employing cybersecurity personnel who must stay current with cybersecurity developments, through education and training, in order to stay aware of changing cybersecurity threats and countermeasures.
5. Creating, implementing, and maintaining written third-party information security policies designed to ensure the security of Information Systems and Nonpublic Information accessible to, or held by, third parties doing business with the Covered Entity. The regulations suggest certain minimum criteria the third-party information cybersecurity policy should address.
6. Creating binding contracts with the third-party service providers which address several contractual provisions suggested by the regulations including, without limitation, use of multi-factor authentication, encryption, certain warranties and representations, and cybersecurity audit rights.
7. Per reporting requirements, issuing at least a bi-annual report, presented to the Covered Entity's BOD (or equivalent governing body) or Senior Officer of the Covered Entity if no such BOD or equivalent body exists, and make a copy of the report available to the DFS upon request. The regulations set forth certain minimum requirements for these reports to DFS.
8. Conducting an annual risk assessment of the Covered Entity's Information Systems based on written policies and procedures. The regulations suggest certain minimum criteria for the risk assessment to include.
9. Upon the occurrence of a Cybersecurity Event, the Covered Entity notifying DFS within 72 hours. Also, on an annual basis (by January 15th), the Covered Entity must certify to the DFS Superintendent the Covered Entity's compliance with the regulations and identify and discuss any cybersecurity weaknesses impacting the Covered Entity and remedial efforts.

There are some limited exemptions to the NY DFS 23 NYCRR 500 regulations. If a Covered Entity qualifies for the limited exemptions, then it shall be exempt from some, but not all, of the compliance requirements of the NY DFS 23 NYCRR 500 regulations. Those Covered Entities meeting all three of the following criteria may qualify for the limited exemptions:

1. fewer than 1000 customers in each of the last three calendar years, and
2. less than $5,000,000 in gross annual revenue in each of the last three fiscal years, and
3. less than $10,000,000 in year-end total assets, calculated in accordance with generally accepted accounting principles, including assets of all Affiliates.

As state and federal regulators continue to evolve their understanding and approaches to cyber threats against the financial services sector (and other sectors), we expect to see them proposing and adopting similar regulations to the proposed DFS regulations (either to supplement or replace existing regulations), as well as proposing other regulations to address the evolving cyber threats and technologies. One such example is the October 19, 2016, proposed rule titled "Enhanced Cyber Risk Management Standards" from the Board of Governors of the Federal Reserve System, the Office of the Comptroller of the Currency, and the Federal Deposit Insurance Corporation.

The bottom line for financial service companies, including banks, insurance companies, other financial services companies, and other businesses, is that you can no longer ignore cyber threats or necessarily take comfort that you have "contracted away" your potential liabilities. Like any business risk, there's no substitute for experience and preparation. Yes, privacy and cybersecurity will require allocation of resources and it will take time, but ignoring cyber threats will ultimately be both more costly and take more time (think crisis when you discover your business has been a victim of a data breach). As Ben Franklin said "An ounce of prevention is worth a pound of cure." It is up to you to decide if you will first confront cyber threats in a preventive or a remedial mode.

WWW.WERNICK.COM – LINKEDIN: http://www.LinkedIn.com/in/alanwernick

