November 14, 2016

***Via electronic submission to*** ***CyberRegComments@dfs.ny.gov***

Maria T. Vullo

Superintendent of Financial Services

New York State Department of Financial Services

One State Street

New York, New York 10004

 **Re: Proposed Cybersecurity Requirements for Financial Services Companies**

Dear Superintendent Vullo:

The Electronic Transactions Association (“ETA”)[[1]](#footnote-1) appreciates this opportunity to provide comments on the New York State Department of Financial Services (“Department”) proposed Cybersecurity Rules for Financial Services Companies (23 NYCRR 500) (the “Proposal” or “Rule”).

ETA is the leading trade association for the payments industry, representing nearly 550 companies worldwide involved in electronic transaction processing products and services. The purpose of ETA is to influence, monitor, and shape the payments industry by providing leadership through education, advocacy, and the exchange of information. ETA’s membership spans the breadth of the payments industry, and includes financial institutions, payment processors, independent sales organizations, and equipment suppliers. ETA’s members use data to provide a wide range of products and services designed to enhance and secure electronic transfers. Our members rely on data to help reduce fraud and to authenticate transactions to make transactions between businesses and consumers seamless and secure.

ETA and its members are dedicated to working with federal and state regulators to address the important and growing issue of cybersecurity. The prevailing cybersecurity best practices developed and implemented in the financial and payments industries are the product of innovation and cooperation between industry and government. We are concerned that the Department’s Proposal may undermine the progress that these federal and self-regulatory efforts have made in combatting cybersecurity threats in the financial industry. First, the introduction of overlapping and potentially conflicting state regulations will cause confusion and compliance challenges for the financial industry. Second, the Proposal’s prescriptive and static rules would likely hinder the ability of institutions to design and calibrate their cybersecurity programs for emerging threats. In contrast, the federal government has long supported a flexible, risk-based approach to cybersecurity, as demonstrated by the National Institute of Standards and Technology (“NIST”) cybersecurity framework, which encourages industry to adapt to ever-changing cyber threats.

To the extent additional cybersecurity requirements are necessary, ETA supports a regulatory approach that provides industry with flexibility to keep pace with innovation in cybersecurity technology and emerging cyber threats. The following provide ETA’s general comments on the Department’s Proposal, as well as specific comments related to the rules set forth in 23 NYCRR 500.

**General Comments on the department’s approach for Cybersecurity in the financial industry**

***ETA Supports a Flexible National Standard for Cybersecurity.*** ETA believes that a flexible national framework is the most effective approach for addressing cybersecurity risks. In the electronic transactions industry, financial information data is governed by federal law, including the Gramm-Leach-Bliley Act (“GLBA”), the Federal Trade Commission’s Safeguards Rule, and robust self-regulatory programs, including the Payment Card Industry Data Security Standard (“PCI-DSS”), which sets forth requirements designed to ensure companies that process, store, or transmit credit card information maintain a secure environment for such data.

Since taking effect in 2003, for example, the information security requirements imposed by the Safeguards Rule have been held up as a model set of elements for developing an information security program. These elements have served as a foundation upon which financial institutions and services companies have built leading cybersecurity programs, leveraging the inherent flexibility of the Safeguards Rule to tailor information security practices and protocols that meet their unique business models, data use practices, and network environments. More recently, in February 2013, President Obama released Executive Order 13636, “Improving Critical Infrastructure Cybersecurity,” which directed NIST to work with stakeholders to “develop a voluntary framework—based on existing standards, guidelines, and practices—for reducing cyber risks to critical infrastructure.” The NIST Cybersecurity Framework, released in February 2014, has seen widespread industry participation, including in the financial industry.

***A Patchwork of State Laws Undermines the Effectiveness of Cybersecurity Programs.*** ETA is concerned that the Proposal will undermine the current, effective federal and self-regulatory framework by encouraging other states to adopt similar, but potentially different cybersecurity requirements, resulting in a patchwork of federal and state requirements for cybersecurity. This approach will force businesses to spend considerable resources interpreting and building compliance frameworks for competing regimes, while also encouraging a “check the box” approach to compliance in place of flexible, agile, and innovative programs.

The development of separate state regimes will not only increase the compliance burden of regulated entities, but also will undermine Federal efforts to develop additional national best practices and standards for cybersecurity. On October 19, 2016, for example, the Federal Reserve Board, the Federal Deposit Insurance Corporation, and the Office of the Comptroller of the Currency issued an advanced notice of proposed rulemaking on Enhanced Cyber Risk Management Standards. The standards would potentially apply to third party service providers. The standards would be tiered, with an additional set of higher standards for systems that provide key functionality to the financial sector. For these sector-critical systems, the agencies are considering requiring firms to substantially mitigate the risk of a disruption or failure due to a cyber event.

If states continue to develop their own cybersecurity regimes, the focus of cybersecurity in the private sector will shift from developing new and innovative best practices to managing and complying with overlapping, or worse, conflicting, state and federal requirements.

***The Proposal’s Prescriptive Requirements Will Limit Flexibility and Innovation.*** The Proposal would add a layer of rigid, prescriptive requirements over an existing federal and self-regulatory framework that favors a flexible and innovative approach capable of quick adjustments to meet evolving cybersecurity threats. The NIST Framework, for example, has been successful largely because it provides private sector entities with a flexible framework for managing and reducing cybersecurity risks, and offers a common vocabulary and approach that is applicable within the financial sector and across various industries. A prescriptive approach to compliance, however, as proposed by the Department, will encourage industry to focus compliance on meeting the regulatory standards instead of risk presented, resulting in a mechanical, rather than dynamic, compliance framework.

**Specific Comments on the Proposed cybersecurity rule**

In the event the Department moves forward with its Proposal, ETA encourages the Department to consider the following specific comments to the regulations in 23 NYCRR 500:

1. The definition of “Covered Entity” in 500.01(c) is overly broad and would subject affiliated companies that are not otherwise under the purview of the Department to potential liability for failing to comply with the regulations. In addition, the regulations should not apply to organizations that are not the large-scale financial institutions, such as money transmitters, captive insurance companies, sales finance companies and service contract providers.
2. The definition of “Cybersecurity Event” is overly broad and would cover minor events and those successfully addressed by a financial institution. Section 500.01(d) should be changed as follows: *Cybersecurity Event* means any confirmed material act ~~or attempt, successful or unsuccessful,~~ to gain unauthorized access to, disrupt or misuse an Information System or information stored on such Information System.
* Not only would it be impossible for a licensee to identify all unsuccessful attempts to access systems, there should be a materiality threshold so that licensees and the Department can dedicate resources to activities that may actually result in loss of customer information or harm to necessary systems. Otherwise, the Cybersecurity Rule would require financial institutions to notify the Department of even the most trivial events involving data that does not present a risk to consumers. This approach would force covered entities to expend significant resources on notification instead of other, more useful compliance efforts, and would force the Department to expend its limited resources reviewing notifications.
1. The definition of Nonpublic Information (“NPI”) is overly broad and would capture data that does not present a risk to consumers if compromised. Section 500.01(g) should be changed by deleting section (4) from the definition of NPI.
* The definition is broader than the GLBA. The definition should track existing federal legislation to reduce burdens on industry.
* As currently drafted, 500.01(g)(4) includes information that “is linkable” even if not currently used to identify a customer. Without limiting the definition to information that is already linked to a customer, any information collected or tracked by a licensee could potentially be included in the definition. Moreover, the inclusion of “information about an individual used for marketing purposes” should be stricken because it could potentially include information created by a licensee based on that customer’s use of the site. Such information would be information that a licensee creates about an individual that is of no use or benefit outside of the licensee’s internal systems.
* This definition is important particularly because of Section 500.15, which requires all NPI to be encrypted at rest and while in transit. To have information that may be, but is not yet, linked to a customer encrypted at rest would impose substantial burdens on licensees and reduce incentives for licensees to innovate using their own internal data derived from customers without any reduction in the impact of a cybersecurity breach on a customer. In addition, the expansive definitions could make it too burdensome to encrypt all such data in transit.
1. Section 500.01(j) should be changed to read: “*Publicly Available Information* means any information that a Covered Entity has a reasonable basis to believe is lawfully made available to the general public.” The remainder of the definition should be stricken.
* As currently drafted, licensees could be deemed to have an obligation to determine whether the source of publicly disseminated information meets the definition. Licensees should not have the burden of determining the source of the information, provided that information was found in the public domain, nor should licensees have the burden of determining whether a particular news source is sufficiently widely distributed to meet the standard. It is impossible for licensees to know distribution of online materials and news sources. Moreover, the definition fails to include information that has been made available to the general public by the individual him or herself.
1. Section 500.04(b) should be clarified so that bi-annually clearly means every two years. To the extent the Department meant twice per year, such period should be revised to be once per year or as frequent as indicated by the company’s risk assessment. Twice per year is unnecessary and out of line with other requirements for annual updates to policies and procedures.
2. 500.05 should be modified so that companies have the flexibility to determine the frequency with which penetration testing and vulnerability assessments are conducted. Considering the broad definitions, the annual requirement for all information systems and non-public information would be too burdensome.
3. Section 500.06(6) requires that records produced as part of the audit trail be retained for six years or more. The regulation should clarify what documents are required to be kept with the audit trail (*i.e.*, whether it is the data logging of all privileged authorized user access or tracking data that allows for complete reconstruction of financial transactions). In addition, the retention requirement should be as long as reasonably necessary, as determined by the organization, in line with the other retention requirement in the Proposal.
* The retention of documents/data that would allow for reconstruction of transactions is all that is needed for a meaningful audit.
* Technology and security systems are continuously being updated and innovated; six years of audit trails would not provide meaningful insight into a program six years later.
1. Section 500.11 requires that a licensee conduct annual audits of third parties to assure they maintain sufficient cybersecurity requirements. The annual requirement should be replaced with a flexible, risk-based standard that allows a financial institution to determine the appropriate audit frequency for each individual service provider. In addition, provision 500.11(b) should clarify that such provisions are recommended but not required based on the licensee’s assessment of the service provider’s risk, and item (4) should be stricken.
* Given the number of service providers that a licensee may deal with and the cost of audits (which often are paid for by the auditing party), an annual audit of each service provider would be extremely burdensome and unproductive.
* It may prove difficult for covered entities to find service providers that are prepared for and able to comply with the requirement that data be encrypted while in transit and at rest. Licensees should have flexibility to work with service providers with security programs that provide sufficient security without having to encrypt data at rest.
* As currently drafted, 500.11(4) could be read to require a service provider to provide and pay for identity protection services in the event of a breach even if there was no compromise to customer financial information. Moreover, it should be left to the licensee and its service provider to determine which party should carry the responsibility of paying for customer service-based remediation in the event of security breaches. This provision should be removed.
1. Section 500.11 should be revised to strike the requirement that a third party service provider represent and warrant that its service or product “is free of viruses, trap doors, time bombs and other mechanisms.” The Department should not interfere in the contractual relations between licensees and service providers. In particular, this provision would force service providers to make an untenable representation and warranty.
2. Section 500.12 should be modified so that multi-factor authentication is not mandated in certain instances, but rather is one of the technological access mechanisms that companies should consider.
* Customers do not universally accept multifactor authentication as a benefit. Many customers view multifactor authentication as a barrier and burden to obtaining services. Licensees should be allowed to implement these safeguards where risks or flags indicate there may be a reason to require additional security or where customers seek additional protection. Licensees, however, should not be required to force the additional burden of multifactor authentication on all customers, particularly where the risk assessment does not indicate it is helpful or necessary.
* Express requirements for multi-factor authentication in all scenarios reduces incentives for innovating new methods of authentication that could be used to safely and accurately ensure customer authentication and identification.
1. Section 500.13 requires destruction of NPI “that is no longer necessary for the provision of products or services”. This language should be changed to “no longer useful for the provision of products or services.”
* In certain cases NPI may not be needed to provide services but is nevertheless useful for fraud prevention or modeling. These uses provide significant customer benefits and improvements to the services, although they may be deemed “unnecessary”. It would harm consumers to require NPI to be deleted when it could otherwise be kept safely and securely to support the licensee’s services.
1. Section 500.15 should be modified to delete the requirement that NPI be encrypted while at rest and in transit in all instances.
* There are numerous technical controls that may be implemented to protect data that are as effective or more effective than encryption. Licensees should have the flexibility to select other methods based on the licensee’s security philosophy and risk assessment.
* A prescriptive encryption requirement limits flexibility. Even if data is not encrypted at rest, licensees could adopt other data security controls to prevent the disclosure of data.
* The Department’s proposal is not consistent with existing standards, including PCI, which requires encryption of data only in transit and not while at rest on a private network. The PCI standard recognizes that there are instances in which clear text access to data at rest must be allowed, including for fraud prevention.
* Requiring encryption of data at rest would reduce licensees’ ability to use such data for fraud prevention. This would harm consumers and offset potential benefits of the requirement, particularly when other security measures can be implemented to prevent disclosure of information while at rest.
1. Section 500.17 should be revised so that (1) notice is only required in the event of actual breaches that materially affect the normal operation of the Covered Entity or that affect NPI, (2) notice is only required within 30 business days, and (3) the certification standard is to the certifier’s knowledge. In addition, the section should clarify the types of documents that should be kept in support of the certification.
* The 72 hour notice requirement is not consistent with any other existing notice requirement. It would be extremely difficult for licensees to provide meaningful notice within that period, as they may not fully understand the impact of a breach within that time period and would not be able to provide meaningful information to the superintendent. Premature notification to customers could cause alarm before all impacts are understood.
* Notice should only be required in the event of confirmed breaches that materially impact the licensee or result in disclosure of NPI (as that definition is modified above). Licensees cannot be expected to know of, let alone provide notification regarding, all attempts to breach the security of their systems.
* Large companies are sometimes the target of unsuccessful hacking attempts that pose no true threat to the licensee or the customer information. Notice of all failed or immaterial attempts would not only cause a burden on the licensee but would inundate the Department with unhelpful information. Both licensees and the Department should focus on areas where harm has actually occurred.
* The form certification states that the “to the best of [Certifier’s] knowledge, the Cybersecurity Program…complies…” The text of the statute in 500.17(b) should conform with this language and state that “the Covered Entity shall submit to the superintendent a written statement by January 15, in such form set forth as Exhibit A, certifying that to the best of the undersigned’s knowledge, the Covered Entity is in compliance with the requirements set forth in this Part.”
* The statement that “Each Covered Entity shall maintain for examination by the Department all records, schedules and data supporting this certificate for a period of five years” is too broad and vague for licensees to follow. It would be impossible for licensees to retain all such information while simultaneously complying with the spirit of 500.13 to destroy all unnecessary (or unhelpful) data. The provision should be revised to require licensees to maintain reports provided to the certifier/Board or Directors and relied upon to support the certification, but should not require retention of all documents that could support such a certification.
1. Sections 500.20 and 500.21 provide that the regulations will be effective January 1, 2017, and that Covered Entities will be required to comply within 180 days from the effective date. The timing for compliance should be extended to 365 days.
* In addition to the practical challenges of meeting the Proposal’s prescriptive requirements, additional time is needed for financial institutions and third party service providers to coordinate their programs and revise their contractual relations accordingly. This is a particular challenge for small and mid-sized companies that lack the leverage when negotiating with larger industry players. These contracts will need to be drafted carefully to address the Proposal’s requirements, and to take into account the lack of clarity over whether covered entities would be held responsible for a third-party’s failure to comply.

\* \* \*

ETA thanks you for the opportunity to submit these comments.

Respectfully submitted,



Scott Talbott

Senior Vice President of Government Affairs

Electronic Transactions Association

1. http://www.electran.org/. [↑](#footnote-ref-1)