

Tech:NYC
Comments to the New York State Department of Financial Services
Regarding Proposed Regulation 23 NYCRR 500
November 14, 2016

Introduction

Tech:NYC represents the technology industry in New York. Our members include more than 300 companies that have a significant presence in New York and range from small startups to large multinational technology companies, banks, and venture capital firms.

As a preliminary matter, our member companies consider cybersecurity to be of paramount importance. We share DFS's rightful concern that New York residents should feel secure in knowing that their private information will be protected. We would like to work with DFS to ensure these regulations are effective but also workable for companies large and small alike.

Compliance with the rule as currently drafted would be extremely burdensome for many businesses, particularly small businesses. We are concerned that the costs and confusion associated with compliance could deter entrepreneurs and business leaders from choosing New York as their company's home, while businesses currently here could choose to move away, and investors may be deterred from investing in New York's technology industry. Moreover, the obligations regarding third parties could deter businesses from contracting with New York-based companies. Ultimately, instead of strengthening New York's place as a global center of commerce, these rules could have the exact opposite of the desired effect and sacrifice New York's place as a top city and state for businesses to make their home. And if companies leave New York for states with lower standards of consumer protection, the rules could have the unintended effect of actually decreasing privacy protections overall.

New York is a pre-eminent place for technology-focused companies and jobs, and technology's importance to the overall economy grows every year. New York consistently ranks among the top states for technology jobs in the U.S.¹ In New York City alone, employment in the technology industry grew at four times the rate of the rest of the economy, and overall employment in technology industry jobs increased 71 percent between 2004 and 2014.² In 2012, the average annual salary for New York City-based workers in the technology industry was \$118,600, compared to an average of \$79,500 for all other jobs in New York City and \$65,400 for all industries excluding the securities industry.³

¹ E.g., CompTIA, "Cyberstates Study for 2015," ranking New York second nationally in new tech jobs for 2015 and for average industry income; and New York State Dept. of Labor "Employment in New York State" (April 2013) referring to NY ranking third in the nation in tech jobs.

² Center for an Urban Future, "New York's Tech Profile" (August 2015)
<https://nycfuture.org/data/nycs-tech-profile>.

³ NYS Comptroller Thomas DiNapoli, "New York City's Growing High-Tech Industry" (April 2014)
<https://www.osc.state.ny.us/osdc/rpt2-2015.pdf>.

In light of the value that the technology industry has to the New York economy, we hope to use this opportunity meet and work together, along with our member companies, to ensure that New York has the highest standards for cybersecurity and continues to be a primary hub for the growing tech sector. Below we have outlined a series of concerns based on input from some of our member companies, including several smaller companies who, as we understand, have not yet interacted with DFS on this issue. While our membership includes both well-established and startup companies, by way of these comments, we hope to provide input on behalf of some of the businesses in New York who otherwise might not have had a voice in the process. We look forward to working with DFS in the coming weeks to identify ways to address these concerns before the subject rule is finalized.

I. General Business Concerns

Effective Date and Deadline for Implementation

The subject rule's effective date of January 1, 2017, and the 180-day window for implementation, is far too short. The rule includes many requirements for which companies will have to dedicate significant time and resources in order to comply (to wit, DFS has advertised these rules as the first of their kind and they will create new obligations for many covered entities). In other circumstances where cybersecurity laws and regulations have been imposed, the relevant authorities allowed reasonable timelines for implementation.

For example, the European Union's General Data Protection Regulation (GDPR) provides more than two years between its passage and effective date.⁴ The U.S. Congress passed the Gramm-Leach-Bliley Act (GLBA) in 1999 but the requirements did not take effect until one year after rule promulgation, in 2003.⁵ Under the federal Health Insurance Portability and Accountability Act (HIPAA), the Department of Health and Human Services released its proposed rule for public comment on August 12, 1998 and did not finalize the rule until February 20, 2003.⁶ HIPAA also allowed more time for smaller health plans to come into compliance with certain provisions of the law.⁷ The Massachusetts legislature passed their current data protection regulations on August 2, 2007. The final regulations were filed February 12, 2009 and ultimately did not go into effect until March 1, 2010.⁸ Notably, the compliance date for these regulations was pushed back several times when it was determined that companies were

⁴ Adopted on April 27, 2016 and effective on May 25, 2018. See, European Commission, "Reform of EU Data Protection Rules" available at: http://ec.europa.eu/justice/data-protection/reform/index_en.htm.

⁵ 16 CFR 314.5(a).

⁶ U.S. Dept. of Health and Human Services "Health Information Privacy: Summary of the HIPAA Security Rule" available at: <https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/>.

⁷ See 45 CFR 164.318, which grants small health plans an additional year to implement certain cybersecurity requirements.

⁸ 201 Mass. Code Regs. § 17 (2009); see also, <http://www.mass.gov/ago/doing-business-in-massachusetts/privacy-and-data-security/standards-for-the-protection-of-personal.html>.

unprepared to meet the requirements within the prescribed time period.⁹ While we understand and share DFS's concern about implementing the rule quickly to avoid any future cybersecurity event, we believe the timeline for implementation needs to be longer to account for the significant changes that covered entities must undertake.

Third Party Obligations

The third-party cybersecurity obligations imposed by the subject rule do not correctly understand business realities, especially for small businesses. First, the rule's third party information security policy would require covered entities to renegotiate contracts with third parties that have access to the information systems and nonpublic information of covered entities within 180 days of the rule's effective date. This requirement is an overwhelming burden within the timeframe provided. At least one of our member companies noted that a business could have literally hundreds of these contracts and there are not enough time and resources for most companies to renegotiate these contracts, assuming that is even feasible, by the date required by the rule. By contrast, when GLBA went into effect, it allowed for a two-year grandfathering of service contracts between covered entities and third parties before the requirements concerning third-party entities went into effect.¹⁰

Second, small and mid-size businesses often lack leverage to persuade third-party companies, especially large ones, to change their cybersecurity policies. Even where a large company does have robust cybersecurity systems in place, it may not share that information with a business covered under this rule. One of our member companies informed us that a large third-party company refused to provide it with details of their cybersecurity compliance because of concerns about sharing proprietary information. Under such a circumstance, a covered entity would be forced to choose between not complying with the rule or terminating third-party contracts, both of which could cause significant business harm. Moreover, the rule requires covered entities to include cybersecurity standards in contracts with third parties, including the authority for a covered entity to audit a third party's cybersecurity system and representations that software is free of viruses. These provisions will be extremely difficult for a smaller company to obtain without significant leverage.

Finally, the subject regulation is ambiguous about whether enforcement for a third party's failure to comply would be directed at the covered entity or that third party. We are concerned that it is not reasonable for a covered entity, in particular a small business, to be held responsible for the actions of a third party.

Recommendations

1. Amend the implementation date to allow covered entities a more reasonable timeframe to implement the rule. One possible way of doing this is to require covered entities to

⁹ Bill Brenner, "Why Mass. 201 CMR 17 Deadline Was Extended" CSO Online (Nov. 24, 2008) available at <http://www.csoonline.com/article/2123439/it-audit/why-mass--201-cmr-17-deadline-was-extended.html>.

¹⁰ See, 16 CFR 314.5(b)

submit cybersecurity plans within 180 days of the effective date and to implement those plans within one year of the effective date.

2. Allow for greater flexibility in the third-party business requirements by identifying other existing cybersecurity laws and standards, such as the National Institute of Standards and Technology's "Framework for Improving Critical Infrastructure Cybersecurity," with which third parties may comply instead of the subject rule.
3. Allow a more reasonable time for covered entities to amend third-party contracts, such as one year for larger entities and two years for smaller ones. Similarly, remove the unreasonable contracting requirements in 500.11(b), including representations about software and the right to audit a third party.
4. Establish a mechanism for DFS to intercede in circumstances when a third-party refuses to provide details of its cybersecurity policy to a covered entity out of concern for trade secrets. One possible way to do so would be to allow those third parties to submit details of its plan to DFS directly to avoid any concerns about sharing proprietary information with other businesses.

II. Concerns Related to Definitions

The Definition of a "Cybersecurity Event"

Defining a "Cybersecurity Event" to include attempted and unsuccessful acts to gain access to an information system makes the notice requirement unworkable. The proposed regulation would currently require covered entities to notify the superintendent of any "Cybersecurity Event," which it defines as any act *or attempt, successful or unsuccessful*, to gain unauthorized access to, disrupt or misuse an information system or information stored on such information system.

Requiring covered entities to notify the superintendent of *attempted* acts aimed at its information system, even when the attempts are unsuccessful, is not feasible. One of our member companies noted that there could be literally thousands of unsuccessful attempts to access its information system in a given day. The administrative burden of reporting all of those attempts would be overwhelming. It also begs the question whether there would be any value for DFS to receive so much information about unsuccessful or attempted acts. Requiring notice of these minor events is far beyond the existing New York State data breach statute, GBS § 899-aa, which only requires notification in the event of an actual "unauthorized acquisition or acquisition without valid authorization of computerized data..." not merely an attempt to acquire such data.

¹¹ It is not clear how covered entities are supposed to follow these divergent definitions. Similarly, the federal HIPAA standard only requires notification to the Secretary in case of a breach, which includes actual "acquisition, access, use, or disclosure of protected health information" and not simple attempts.¹²

¹¹ See, GBS § 899-aa(1)(c) (defining a "[b]reach of the security of the system" and noting that in determining that an unauthorized acquisition has been made, a business may consider factors that demonstrate the data is in the possession of or has been downloaded or used an unauthorized person).

¹² 45 CFR 164.402; 45 CFR 164.408.

The Definition of “Nonpublic Information”

The definition of “Nonpublic Information” is overly broad, covering more information than the federal regulations do and capturing more information than is necessary for the effectiveness of the rule. As it is currently written, the proposed rule would capture most information used internally by businesses that is not personal, cannot be used to identify an individual and poses no material harm to any person in the event of a breach. For example, the rule defines nonpublic information to include, in part, “[a]ny business related information...that would cause a material adverse impact to the business, operations or security of the Covered Entity.” Put in context, while an unauthorized disclosure of a covered entity’s trade secrets would materially impact such entity’s business, the means used to protect such trade secrets should not be within the purview of DFS. In addition, the definition may capture information maintained by businesses in aggregate form only and separate from identifiable elements. Such non-identifiable data is vital to many New York startup companies’ ability to quickly scale, grow, and improve their products and services. Coupled with the proposed rule’s strong encryption requirements, this imposes undue obligations on covered entities.

Clarifying the Meaning of “Covered Entities”

The proposed rule is not clear about what specific business services it aims to regulate. While the rule defines a “Covered Entity” to mean any person “operating under or required to operate under a license, registration, charter, certificate, permit, accreditation or similar authorization” under the state’s banking, insurance or financial services law, it is not clear what particular business practices the rule actually aims to address. In conversations with a variety of stakeholders we have heard significant confusion about to whom the rules apply, and whether certain exemptions exist for certain industries. In one conversation, we were told that the rule will not apply to health insurance companies. But that fact is not evident based on a plain reading of the rule. This type of uncertainty presents significant challenges to businesses in New York.

Recommendations

1. The definition of “Cybersecurity Event” should be narrowed significantly to only include *successful* efforts to gain unauthorized access to a covered entity’s information system.
2. The definition of “Nonpublic Information” should be narrowed to only include personally identifiable information (PII) or information that can be used to identify an individual.
3. DFS should clearly specify the types of services covered by the proposed rule and explicitly identify any exemptions that exist for any of the sanctioned businesses.

III. Technical Concerns

Cybersecurity Event Notice Requirement

There are several concerns about the 72-hour notice requirement. First, the 72-hour window is unreasonably short. Several of our members indicated that they could still be trying to determine

the facts surrounding an actual cybersecurity event within 72 hours of discovering its occurrence. A 72-hour deadline could interfere with a reasonable and thorough investigation of an incident and cause a covered entity to rush to an incorrect conclusion. Moreover, as one observer noted, the 72-hour notice requirement would likely require businesses to have cybersecurity incident response personnel in place 24 hours a day, 365 days of the year.

Second, the standard for providing notice is vague and will likely lead to confusion. The rule requires covered entities to notify the superintendent of any cybersecurity event that has a *reasonable likelihood of materially affecting* the normal operation of the covered entity or that affects nonpublic information.¹³ Covered entities may not actually know when a threat has a reasonable likelihood of materially affecting its normal operations—this is a vague standard that will likely leave businesses confused about when to report an incident.

Third, the notice requirement does not specify how a covered entity must report any such cybersecurity event. Without further guidance, covered entities will be forced to guess—during the already very brief 72-hour notice period—as to what specific information DFS requires regarding a cybersecurity event. We are further concerned that a covered entity could be subject to fines or other enforcement action if DFS is not satisfied with the amount of information it provides regarding a cybersecurity event.

The 72-hour notice requirement seems unreasonable when compared with similar federal and state requirements. HIPAA, for example, allows a covered entity up to 60 days after discovery of a breach to provide notification to the Secretary. Notably, the New York State data breach statute does not even set forth an explicit notification deadline. Instead, the statute only requires an entity to disclose a breach “in the most expedient manner possible and without unreasonable delay,” thereby allowing the affected entity to disclose the event on a more realistic timeline.¹⁴ To put this standard in context, states that have specified notification deadlines in their data breach statutes have pegged them at 15-60 days following discovery of the breach and not anywhere near the 72-hour deadline proposed by DFS.¹⁵

Finally, the notice requirement appears to have two different, and potentially confusing, triggers. In addition to requiring notice to the superintendent of a “cybersecurity event” in 500.17(a), the proposed regulation also requires, in 500.17(b)(2), notice to the superintendent within 72 hours of any “material risk of imminent harm relating to its cybersecurity program.” It is not clear how, if at all, such a material risk of imminent harm differs from a cybersecurity event as there are no definitions to guide covered entities as to its meaning.

Certification of Board Chair or Senior Officer

The proposed rule’s requirement that each covered entity submit an annual statement of compliance to the superintendent could subject a covered entity’s board chair or senior officers

¹³ 500.17(a)

¹⁴ GBS 899-aa(2).

¹⁵ See, e.g., <http://www.dwt.com/statedatabreachstatutes/>.

to civil or criminal liability. We feel strongly that imposing this type of penalty on an individual for actions related to a compliance certification is far too high of a penalty and could discourage business leaders from incorporating in New York or discourage individuals from serving on the boards of covered entities.

Recommendations

1. Amend the notice requirement to a more reasonable timeframe such as the 60-day requirement for HIPAA or the “most expedient manner possible” standard from the New York State data breach statute. If the agency remains concerned about receiving notice as quickly as possible, it should require a simple notification, and nothing more, within 72 hours, and require covered entities to provide additional details as soon as they become available.
2. Eliminate the vague standard of requiring notice when a cybersecurity event has a *reasonable likelihood of materially affecting the normal operation*. Instead only require notice if a cybersecurity event results in the unauthorized acquisition of nonpublic information.
3. Clearly set forth the notice requirements for covered entities to report a cybersecurity event, and ensure that those notice requirements are as minimal as possible to ensure that the covered entity will devote as much of its resources to addressing the cybersecurity event.
4. Eliminate the confusing and duplicative notice requirement in 500.17(b)(2) for “material risk of imminent harm relating to [a] cybersecurity program.”
5. Establish reasonable penalties for failing to comply with the terms of the rules and eliminate any possible personal liability for board chair or senior officers related to the annual compliance certification.

Conclusion

We respectfully request that DFS amend the proposed rule based on the foregoing concerns and recommendations. We welcome the opportunity to meet to discuss these items further at your earliest convenience.