Comments of the Center for Economic Justice and Peter Kochenburger

To the NAIC Cybersecurity Model Law Draft Group

April 17, 2017

The Center for Economic Justice (CEJ) and Peter Kochenburger submit the following comments on three topic: (1) general comments on the third version of the draft Data Security Model law; (2) the proposal to bifurcate the draft into two parts, presumably pre-breach data security requirements and post-breach notification and consumer protection standards; (3) adopting New York Department of Financial Services (DFS) Cybersecurity Regulations as a substitute for sections of the current draft.

1. Comments on the Working Group's Third Draft.

From the discussion in Denver, it appears the Working Group is considering limiting the draft Data Security Model Law to the data security sections while separating or deleting the post-breach requirements. The Working Group is also considering the New York DFS Cybersecurity Regulations as a substitute for much or all of the current draft. Based on the discussion in Denver, we limit our comments on version 3 of the draft model to general comments. We can provide more detailed comments and textual revisions on this version as needed.

Improvements in Version 3:

- While the exemptions in Section 2.B are overly broad, the addition of "that provides at least as much protection as this Act" helps address our concern that this section would allow many regulated entities to avoid complying with the provisions of the NAIC model.
- Utilizing the taxonomy "data breach" and "data breach without use of personal information."
- The addition of the last sentence in Section 4.A: "This documentation shall occur whenever any substantive changes to the Information Security Program occur but not less than on an annual basis."
- Utilizing "Best Practices" in section 4.D.(1) (b).
- Section 5.D, Notification to the Commissioner," clarifies this important section.
- The provision at the end of Section 6.C requiring Commissioner review of draft notices is a good idea and we encourage the Working Group and licensees to develop these notices utilizing best practices in drafting consumer disclosures, including consumer testing. This should also substitute for the vague "plain language" requirement immediately following this paragraph.
- Simplifying Section 12 to reference existing state laws on the departments' regulatory authority.

Ongoing or New Problems with Version 3:

- Section 2 no longer contains the provision that a state law is not considered "inconsistent" with the Act if it offers greater protection to consumers.
- Section 4.F removes the crucial protection that licensees are responsible for their third-party service providers' failures to protect personal information provided to them by the licensee. As discussed in earlier comments, this provision places the responsibility for third-party data breaches on the party best able to police the service provider, which is the licensee who selects, pays and oversees these vendors – as opposed to the consumer, who has no comparative role.
- The Confidentiality provisions in Section 10 are essentially unchanged and are unnecessarily broad – please see our earlier comments, along with those filed on the first draft by several state insurance departments.
- The sixty-day window for notification to consumers of a Data Breach in Section 6 is excessive.
- The provision in Section 6.C(2) stating notification requirements under other state laws can satisfy the provisions in this Act is inconsistent with the Act's intent to provide consistent ("exclusive") data security protections for individuals affected by a data breach.

In addition, we suggest that a provision be added to the Cybersecurity Model Law to require public disclosure of insurer performance of the cybersecurity requirements of the model law. Publication of insurers' cybersecurity performance provides crucial information to consumers as they decide which insurer or producer to whom they will entrust their personal information. In addition to relying on market forces to encourage stronger cybersecurity by insurers, publication of insurer cybersecurity performance – how well insurers and licenses are meeting the cybersecurity requirements of the model law – will bring essential transparency and accountability of regulators' oversight of licensees' cybersecurity practices. Insurer performance could created without jeopardizing proprietary information by using a rating system – say 1 to 10 – for each of the key deliverables in sections 4, 5 and 6.

2. Bifurcating the NAIC Draft pre-breach and post-breach requirements.

Combining pre-breach data security requirements with post-breach notification and consumer protection standards provides a more comprehensive model, enhances consumer protection, and better advances consistency in this area among the states. It is also consistent with the NAIC Roadmap for Cybersecurity Consumer Protections. We prefer a model act that addresses these issues comprehensively. However, consensus requires some compromises, which we have not seen yet from industry. Industry should not be rewarded for refusing to move off of unreasonable positions.

A primary concern with bifurcation of the model is that the financial regulation aspects of the model will proceed while the consumer protection aspects will never materialize. If the industry will not agree to important consumer protections now, what makes regulators think industry will ever agree to such protections in the future – when industry's failure to compromise to date has apparently produced the desired goal of stripping consumer protections from the model law? We look to the regulators on the drafting group to reject unreasonable industry objections to produce a balanced approach which includes critical consumer Cybersecurity protections in the model law.

3. Adopting the New York DFS[1] Cybersecurity Regulations (23 NYCRR 500).

On April 9, 2017 at the NAIC spring meeting in Denver, New York Superintendent of Insurance and Banking Maria Vullo summarized the New York Department of Financial Services' recently promulgated Cybersecurity Regulations for regulated entities, including insurance companies and producers. Superintendent Vullo also suggested that the NAIC base its Insurance Data Security Model on the New York Regulations rather than continue a separate drafting effort. Rhode Island Director of Insurance Elizabeth Dwyer, who chairs the NAIC's Cybersecurity ad-hoc drafting group, then requested interested parties to comment on this suggestion.

Perhaps the primary advantage in using the New York Cybersecurity Regulations (Regulations) as a model is that they have already been developed and adopted by the state regulator responsible for supervising the most important financial services center in the United States, including solvency oversight of the largest insurance premium volume in the country. These Regulations went through several drafts and numerous opportunities for notice and comment, presumably by many of the same interested parties also participating in the NAIC's model drafting process. We do not assume this process means the Regulations necessarily provide the best balance of data and consumer protection and minimizing regulatory burdens, but utilizing them may significantly advance the utility and speed of the NAIC's drafting process for its own Data Security Model, as well as promote uniformity in state insurance regulation in this area.

The New York Regulations appear to provide more robust protections in several areas. These include a more specific testing and vulnerability assessment, requiring an "audit trail,"[2] and avoiding the broad HIPAA exemption in the NAIC Draft.[3] While earlier drafts of the NAIC model provided more adequate safeguards in licensee use of third-party service providers than the New York Regulations, the third draft waters these down considerably.[4] The Confidentiality provisions in NY Regulation Section 500.18

---

[1] Compare NY Regulation § 500.05 with NAIC Draft Section 4.D.(2)(f).
[2] NY Regulation § 500.06.
[3] NAIC Draft Section 2.B – HIPAA is just one of the exemptions possible under this section. Note that the Third Draft limits this exemption to federal laws that "provides at least as much protection as this Act," which is an improvement over the previous draft.
[4] NAIC Draft Section 4.F appears to weaken the Cybersecurity standards required of third-party service providers and more significantly, removes the provision holding licensees responsible for

are broad but do not appear to expand confidentiality beyond existing provisions in New York Insurance, Banking, and related laws. In contrast, Section 10 in the NAIC Draft arguably exempts more information from public access than existing laws would provide.[5]

Sections 5-8 of the NAIC drafts contain detailed provisions for notifications of a data breach to Insurance Commissioners (Section 5.D) and consumers (Section 6.C), and significant flexibility for regulators to "prescribe the appropriate level of consumer protection required following the Data Breach" (Section 7). In contrast, the New York Regulations do not directly set out consumer notification requirements, do not specify the information that must be provided to the regulator, nor provide the enforcement flexibility to the Superintendent set out in the NAIC drafts.[6]

Consumer notification requirements and the minimum levels of consumer protections required after a Data Breach of Personally Identifiable Information are very important. While the New York Regulations do not explicitly address consumer notification requirements, DFS' "Frequently Asked Questions" to this regulation state:

> 2. Is a Covered Entity required to give notice to consumers affected by a Cybersecurity Event?
>
> New York's information security breach and notification law (General Business Law Section 899-aa), requires notice to consumers who have been affected by cybersecurity incidents. Further, under 23 NYCRR Part 500, a Covered Entity's cybersecurity program and policy must address, to the extent applicable, consumer data privacy and other consumer protection issues. Additionally, Part 500 requires that Covered Entities address as part of their incident response plans external communications in the aftermath of a breach, which includes communication with affected customers. Thus, a Covered Entity's cybersecurity program and policies will need to address notice to consumers in order to be consistent with the risk-based requirements of 23 NYCRR Part 500. http://dfs.ny.gov/about/cybersecurity_faqs.htm.

---

harm caused by the licensee's service provider's data breach. NY Regulation § 500.11 sets out third party service provider requirements.

[5] We commented on the draft Confidentiality provision in our February 16, 2017 comments to the ad-hoc drafting group (pp. 11-12).

[6] This may simply be a drafting preference rather than a real difference in regulatory authority between the NY Regulations and the NAIC model.

New York General Business Law § 899-aa states in part:

> Any person or business which conducts business in New York state, and which owns or licenses computerized data which includes private information shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the system to any resident of New York state whose private information was, or is reasonably believed to have been, acquired by a person without valid authorization. The disclosure shall be made in the most expedient time possible and without unreasonable delay … New York Business Law § 899-aa.2.

Presumably, therefore, this requirement is implicit in the New York Regulation and DFS-regulated entities, including insurers and insurance producers, must notify all consumers whose private information may have been accessed. And, they must do so "in the most expedient time possible," rather than the 60-day notification requirement contemplated by the NAIC draft. There also does not appear to be a harm trigger.

Should the NAIC adopt the New York Regulation as its model, the major issue becomes the consumer notification requirement. Options include omitting any reference at all, a provision incorporating the notification laws of the state adopting the model, or inserting the New York notification requirements in New York General Business Law § 899-aa directly into the NAIC model.

We strongly prefer the last option, which would provide a robust and uniform notification requirement for insurance consumers throughout the country and ensure that when their information is impermissibly accessed from a third party licensee, they will be aware of it and able to make the decisions themselves as to whether the breach was "material" and what if any remedial steps should be taken. The second option – incorporating existing state laws – would return us to the status quo and insurance consumers would have no more rights in this area than they do now, and the advantages of uniformity only partially filled. However, this option is preferable to the first, which at best adds considerable uncertainty about consumer notifications and remedies, and at worst could create an argument that other state notification requirements are preempted by this model, creating a regulatory void for insurance consumers.

The New York regulation does not include any provision for publication of licensee performance of the cybersecurity requirements. As discussed above, publication of such performance outcomes is a reasonable and necessary tool for accountability of regulators and insurers to, and empowerment of, consumers who face a choice of which insurers and producers to whom they will entrust their personal information.