NATIONAL CONFERENCE OF INSURANCE LEGISLATORS
FINANCIAL SERVICES AND INVESTMENT PRODUCTS COMMITTEE
NEW ORLEANS, LOUISIANA
MARCH 4, 2017
DRAFT MINUTES

The National Conference of Insurance Legislators (NCOIL) Financial Services and Investment Products Committee met at the New Orleans Downtown Marriott on Saturday, March 4, 2017 at 8:15 a.m.

Senator Bob Hackett of Ohio, Chair of the Committee, presided.

Other members of the Committee present were:

Rep. Sam Kito, AK
Sen. Jason Rapert, AR
Sen. Travis Holdman, IN
Rep. Joseph Fischer, KY
Rep. Jeff Greer KY
Rep. George Keiser, ND
Asm. Will Barclay, NY
Sen. James Seward, NY

Other legislators present were:

Rep. Steve Riggs, KY
Rep. Matt Lehman, IN
Rep. Lois Delmore, ND
Sen. Nellie Pou, NJ
Asm. Kevin Cahill, NY

Also in attendance were:

Commissioner Tom Considine, NCOIL CEO
Paul Penna, Executive Director, NCOIL Support Services, LLC
Will Melofchik, Legislative Director, NCOIL Support Services, LLC

MINUTES

Upon a motion made and seconded, the Committee unanimously approved the minutes of its November 17, 2016 meeting in Las Vegas, Nevada.

UPDATE ON NAIC INSURANCE DATA SECURITY MODEL LAW

Birny Birnbaum from the Center for Economic Justice (CEJ) stated that CEJ thinks it is extremely important for NAIC to draft this Model because it strives to set out basic goals and requirements for insurers regarding data security which is fundamental for consumer protection and financial regulation. It is an integral part of monitoring the company's solvency because the data security issues relate to the company's operations and data breaches can have a significant financial impact on the company. The first part of the Model deals with financial regulation issues such as what kind of requirements companies have for data security and what kind of responsibilities they have in terms of monitoring those responsibilities. The second part of the Model deals with market regulation and consumer protection issues such as defining what a data breach is, and defining what to do in the event of a data breach.

One contentious issue from CEJ's perspective is that there is great flexibility in the Model given to financial regulators in terms of how they apply the various standards but when it comes to the consumer protection aspects of the Model, the insurers and licensees have been demanding total uniformity with low consumer protections. Mr. Birnbaum stated that CEJ believes that a fundamental consumer protection is notifying consumers if their personal information has been lost or stolen and the argument that notifications to consumers will lose their "power" if consumers are inundated with them does not hold merit – if your information is lost or stolen, your only tool to protect yourself is to be alerted in the first place. Accordingly, CEJ is opposed to the "harm trigger" in the Model that gives the insurance company/licensee discretion to decide what will or won't harm the consumer. CEJ believes there is no way that insurance companies and licensees can know the particular circumstances of when a consumer is harmed. CEJ asked for examples of data breaches that did not harm consumers and the examples were all instances where the data was not actually breached – information was sent to the wrong lab or released to the wrong agency and then recovered without use/distribution by that third party. CEJ suggested that if you can demonstrate that the lost data was recovered without further distribution, that is not a data breach. Mr. Birnbaum stated that the current draft of the Model is nowhere near being a finished product but urged NCOIL to support it going forward.

Frank O'Brien from the Property Casualty Insurers Association of America (PCI) stated that yesterday's NCOIL – NAIC Dialogue was very instructive in that we heard doubts from Commissioners regarding the effectiveness of the Model drafting efforts thus far. These are constantly evolving issues, made more interesting by the recent issuance of the New York Department of Financial Services Cybersecurity Regulations. Mr. O'Brien stated that where NAIC and the industry ends up with the Model is open to debate. Sen. Hackett agreed and stated that he is part of a cybersecurity task force in Ohio and there are so many competing interests to deal with. Rep. Lehman stated that it is hard to deal with these issues without actuarial data and how the standards in the Model can be applied to other industries. Mr. Birnbaum stated that the Model isn't about developing cyber liability policies, it's about protecting data and protecting consumers in the event of a data breach. The issue of developing cyber liability policies and promoting a cybersecurity market is vitally important but separate from the Model. Rep. Lehman agreed but stated that the adoption of the Model creates a need because if the Model is adopted, a carrier or agent will realize that if they don't comply they can experience a loss and will therefore go to the market to see what there is to fill gaps. Sen. Hackett agreed.

Kate Kiernan from the American Council of Life Insurers (ACLI) stated that ACLI supports the NAIC's drafting efforts primarily because of the need for uniformity - the 47 different State data breach requirements is not workable. At the Federal level, there has been a lack of movement due to competing interests. Due to that lack of movement, it was thought that starting with the NAIC, because of the members' knowledge and expertise in the industry, would be prudent. In response to one of Mr. Birnbaum's earlier comments, Ms. Kiernan stated that ACLI is not pushing for a lower consumer notification standard – ACLI wants any notification to be meaningful so that consumers take it seriously.

Eric Cioppa, Superintendent of the Maine Bureau of Insurance, stated that Maine is heavily involved with efforts in trying to improve the Model. Supt. Cioppa stated that drafting has proved difficult because of the competing interests but he is optimistic of the

drafting efforts moving forward. Supt. Cioppa welcomed a call with NCOIL to review the current draft and noted that States need to monitor very closely what insurers are writing and what the amounts are for cyber liability policies.

Joe Thesing from the National Association of Mutual Insurance Companies (NAMIC) stated that NAMIC believes that the recent draft of the Model is headed in the wrong direction. Regarding the harm trigger, in the current draft of the Model, if there was a breach to my auto insurance policy and the only thing exposed was my home address, that would trigger all of the notice provisions of the Model, and not just for him but for all the policyholders in the company – that is concerning.

Wes Bissett from the Independent Insurance Agents and Brokers of America (IIABA) stated that the Model is very broad in that it applies to insurance companies and also to insurance agents and brokers. On the other hand, it is very narrow in that it only applies to the insurance industry. The Model has two main components: a set of data security standards that outline how to protect data; and what happens if you think or find out there was a breach. The latter is controversial. Mr. Bissett stated that if the Model were to be enacted, most agents would have to hire an outside vendor to help them develop the data security requirements, and would also have to purchase a cyber liability policy – those costs are significant. There is an inherent tension in the Model: on one hand, it's insurance specific and on the other hand NAIC wants the Model to expand to relationships insurers have with third parties. Mr. Bissett asked how can small agents compel much larger third party vendors to do anything? IIABA has suggested that third parties should have direct obligations but that would broaden the scope of the Model and not make it insurance-specific. The Model also makes an independent agent responsible to investigate after a company breach – that is impractical. IIABA has suggested that the NAIC narrow its focus on the first part of the Model – the set of data security standards, since 47 States already have data breach notification standards. In fact, Supt. Cioppa's Financial Condition Committee has recommended that approach. That is what New York did – it adopted regulations that did two core things: it addressed information security standards and then addressed a regulatory gap in that most States don't require licensees to notify regulators when there has been a breach. IIABA believes those two components together could form a strong Model that it could support.

Rep. Joseph Fischer (KY) asked if the Model is adopted, do we need to preempt existing cybersecurity laws applicable to companies? Mr. Birnbaum stated that is an issue that has been discussed extensively. The industry position is yes, it has to preempt everything else and the consumer perspective is that it should be a minimum standard – if a State has a higher standard, that higher standard applies. Mr. Birnbaum also stated that the Model is important because if an all-industry Model is drafted, that may work on the consumer protection side but not on the regulator side – regulators need industry specific data security requirements because the insurance industry is different from other industries. Ms. Kiernan agreed. Rep. Fischer asked, under current law, who has standing to enforce the laws and who has standing to enforce the Model? Mr. Bissett stated that the insurance department would enforce the Model and Attorney Generals typically enforce other laws. Rep. Fischer asked if there is a private cause of action accounted for in the Model? Mr. Bissett noted that the Model states that if a private cause of action existed prior to the Model, then it would continue to apply. Mr. Birnbaum stated that CEJ proposed there should not be a private cause of action for any financial regulation related issues but there should be one for the consumer protection aspects, particularly if there is a harm trigger.

DISCUSSION ON RESOLUTION IN SUPPORT OF AN EXEMPTION FOR COMMUNITY BANKS FROM ONEROUS AND UNNECESSARY REGULATIONS

Sen. Travis Holdman (IN) stated that in today's financial world, small banks are completely overwhelmed by Dodd-Frank compliance and that has led to more and more consolidation in the market. Community banks are the heart of what goes on in most communities around the country. Accordingly, the Resolution asks for community banks (less than $10 billion in assets) to be exempt from the onerous and unnecessary CFPB regulations. Sen. Holdman stated that he hopes the CFPB is abolished but if not, community banks should be exempt from its regulations in order to thrive and benefit local communities.

Sen. Hackett agreed and stated that community banks have suffered from the costs of compliance. Sen. Hackett asked if there were any new developments in D.C. about Dodd-Frank reform? Kevin McKechnie from the American Bankers Association (ABA) stated that he supports Sen. Holdman's Resolution and that consolidation is an economic enemy. There are more people trying to enforce rules than there are trying to lend and create credit – that is not going to grow the economy. One Federal development is the Financial CHOICE Act which contains meaningful changes but the question remains whether it will become law.

Rep. Steve Riggs (KY) stated that he never understood why Dodd-Frank applies to all banks because it was only the large banks that engaged in the risky practices such as credit default swaps. Rep. Riggs asked why $10 billion is the "trigger" in the Resolution - why can't the trigger be the specific activities the bank conducts. Sen. Holdman stated that under industry standards, less than $10 billion in assets is regarded as the point which you are considered to be a community bank. Commissioner Tom Considine, NCOIL CEO, stated that the $10 billion trigger also comes out of Dodd-Frank. There is an exemption in Dodd-Frank at the $10 billion level and the CFPB has a "no-exam" rule at the $10 billion level. Cmsr. Considine further stated that community bankers were and are told by CFPB examiners: "don't worry about the regulations, we won't examine you." However, being responsible business people, community bankers nevertheless hire expensive compliance officers.

Mr. Birnbaum stated that CEJ opposes the Resolution. First, compliance for community banks isn't completely a result of the CFPB – increased compliance is mostly due to their specific regulators. Second, the decline in the number of community banks is a long-term trend not necessarily associated with Dodd-Frank/CFPB. Third, the Resolution is too broad and it would be anti-consumer to prohibit a consumer protection agency from regulating community banks. Lastly, Mr. Birnbaum stated that the CFPB has done great things for consumers and has a lot of value. Sen. Holdman disagreed and stated that we don't know how well community banks could have performed due to the all the regulations and associated compliance costs. Also, another issue that arose from Dodd-Frank is that of capital requirements. Unnecessarily raising capital requirements means that banks have less money out in their communities loaned to those seeking to start a business, buy a home, or buy a car. Sen. Holdman also agreed with Cmsr. Considine's earlier comments and requested that the Committee not vote on the Resolution so it can be further discussed at the Summer Meeting in Chicago. Sen. Jason Rapert (AR) asked Mr. Birnbaum what has the CFPB actually done and stated that he has frequently been told by community bankers in Arkansas that the CFPB tells

them to ignore standards and write-off bad loans. That does not seem like consumer protection. Mr. Birnbaum first stated that the CFPB is the wrong target of this Resolution and then stated that he can't speak to specific instances in Arkansas, but that the CFPB has recovered billions of dollars for consumers from unfair and deceptive practices.

DISCUSSION ON NEW YORK, OTHER STATE, AND FEDERAL CYBERSECURITY DEVELOPMENTS

Aaron Tantelff, Esq., Foley & Lardner, LLP, stated that the New York regulations became effective on March 1, 2017, and that covered entities must comply with most requirements by August 28, 2017. The regulations have a broad applicability despite the exemptions contained therein. The exemptions only exempt certain provisions such as penetration testing, audit trial, encryption, and incident response plan rules. Mr. Tantleff noted that he thought the incident response plan exemption was strange. Rep. George Keiser (ND) asked if there was a lot of discussion from small employers regarding the "less than 10 employees or less than $5 million in gross annual revenue" exemption. Mr. Tantleff stated that there were several comments on that issue but he got the impression that the NY DFS simply stated "thank you for your comment, but we are moving forward." Mr. Tantleff further stated that the initial draft was a one-size-fits-all approach, and that he thinks the exemptions are extremely narrow.

Mr. Tantleff stated that when he works with companies in trying to figure out how to comply with these regulations, there are some concerns. For instance, in Section 500.06, audit logs must be designed to "reconstruct material financial transactions sufficient to support normal operations and obligations of the Covered Entity." The questions become: what does that mean? who determines what that includes? And the same section requires the logs to be designed to "detect and response to cybersecurity events that have a reasonable likelihood of materially arming any material part of the normal operations of the covered entity." Those sections represent a double-materiality standard and make compliance difficult. Additionally, section 500.12 requires multi-factor authentication which is a great idea in theory but has proven to be difficult to comply with. Additionally, the requirements in Section 500.13 regarding data retention make it difficult to have adequate fraud detection. The double notification trigger under Section 500.17(b) is also very difficult to understand. Section 500.18 regarding confidentiality also raises concerns about making disclosures about vulnerabilities of an organization.

The regulations also require the CISO to report in writing at least annually to the board of directors or its equivalent. Under the NAIC Model, there is no indication as to where the report goes. Mr. Tantleff noted that the 72-hour notice requirement in the New York regulations is difficult to comply with, because of the time limit and because of deciphering what "reasonable likelihood of materially harming any material part of the normal operations" means. Regarding third-party service providers, Mr. Tantleff stated that he thinks they play a huge role in terms of risk to the organization. The companies need to be required to do their due-diligence before contracting with them and the third-party service providers need to be held accountable as well. Mr. Tantleff then noted some differences between the New York regulations, the Gramm-Leach-Bliley Act, and the Federal Financial Intuitions Examination Council such as notification requirements, encryption, and covered information. Mr. Tantleff closed with saying that he supports uniformity in cybersecurity/data breach requirements and acknowledged there is a lot of work to do.

Ron Jackson of the American Insurance Association (AIA) stated that the New York regulations represent a persistent problem – lack of uniformity. Mr. Thesing stated that its important to note that what New York did are regulations, not legislation. Accordingly, legislators didn't debate and weigh in on them. NAMIC opposed their efforts. Ms. Kiernan stated that ACLI is concerned about the notice requirements in the New York regulations and that in 2017, ACLI is tracking 17 pieces of State cybersecurity legislation. It seems that the "patchwork" of requirements relating to cybersecurity will continue to grow and ACLI supports a uniform standard. Mr. McKechnie stated that he will be delivering a PowerPoint presentation in Ohio that he would be happy to make available to this Committee. Mr. McKechnie further stated that passing regulations without an understanding of the technology at issue is a bad way to handle this. Lastly, he stated that State legislators need to find a way to get security clearances because as it stands, none can get the briefings required to understand what really is going on with cybersecurity.

ADJOURNMENT

There being no further business, the Committee adjourned at 9:45 a.m.