NATIONAL CONFERENCE OF INSURANCE LEGISLATORS
FINANCIAL SERVICES COMMITTEE
CHICAGO, ILLINOIS
JULY 15, 2017
DRAFT MINUTES

The National Conference of Insurance Legislators (NCOIL) Financial Services Committee met at the Chicago Intercontinental Magnificent Mile Hotel on Saturday, July 15, 2017 at 10:15 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
Asm. Ken Cooley, CA
Sen. Travis Holdman, IN
Rep. Joseph Fischer, KY
Rep. Jeff Greer, KY
Rep. Bart Rowland, KY
Rep. Greg Comer, LA
Rep. George Keiser, ND
Sen. Jerry Klein, ND
Rep. Don Flanders, NH
Rep. Bill Botzow, VT
Rep. Kathie Keenan, VT
Sen. Mike Hall, WV
Del. Steve Westfall, WV

Other legislators present were:

Rep. Deborah Ferguson, AR
Rep. Austin McCollum, AR
Rep. Matt Lehman, IN
Rep. Willie Dove, KS
Rep. Lana Theis, MI
Rep. Lois Delmore, ND
Asw. Maggie Carlton, NV
Rep. Marguerite Quinn, PA

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 March 3, 2017 meeting in New Orleans, Louisiana.

NY DFS CYBERSECURITY REGULATIONS: A NATIONAL BLUE PRINT?

Maria Filipakis, a Managing Director at Global Atlantic Financial Company and former Executive Deputy Superintendent at the New York Department of Financial Services (NY DFS), stated that while developing the cybersecurity regulations during her time at the NY DFS, she and her staff were tasked with highlighting and detecting emerging risks and threats to the different kinds of entities the NY DFS regulates which includes banks, insurance companies, money transmitters, and check cashers. Ms. Filipakis stated that they quickly determined that cybersecurity was one of the most critical risks that the NY DFS had to deal with. There was an increased sophistication of attacks, an increased connectivity in the financial network, and people's financial lives were online more than ever before due to online banking. The NY DFS sent out

surveys in 2013 and 2014 to regulated entities, ranging from credit unions and community banks, to all types of insurers, in an effort to gain more information from them regarding their cybersecurity problems and protocols. On the insurance side, they found that personally identifiable information (PII) and protected health information had an increased value on the black market.

Ms. Filipakis stated that the survey consisted of highly technical questions on topics such as the types of computer security in place, to questions on their corporate governance regarding: board of director knowledge of cybersecurity; what type of mitigation factors did the institution already have in place such as incident response plans, security protocols, and cyber insurance; how much of their budget was allocated to cybersecurity; was it considered a real risk or simply allocated to the IT department; what were their future plans. From the responses to the survey the NY DFS was able to gather general conclusions such as that there were varying levels of preparation based on the types of business lines the entity had, how many transactions they engaged in, and their marketing opportunities. This led to the NY DFS expanding the focus of its IT exams to include an increased focus on cybersecurity, and educating financial institutions on their increased reliance on third party service providers.

Ms. Filipakis stated that the NY DFS then met with several state and Federal agencies, stakeholders, and industry representatives and ultimately issued the regulations for comment. After extensive feedback, there were adjustments made and it went into effect this past March. The regulation requires, among other things, a risk-based approach, and the purpose of the regulations was to make sure the NY DFS was safeguarding consumer information, and the information systems of the entities themselves. There is a requirement that all entities put together a cybersecurity program that is in line with that set forth by the National Institute of Standards and Technology (NIST). Additionally, companies must conduct a risk assessment, matched to their business plans, and create cyber policies which involves designating a Chief Information Security Officer (CISO) – for smaller entities, that function can be outsourced. Companies also must come up with an incident response plan; make determinations as to whether multi-factor authentication and encryption of non-public information is necessary and if not, whether or not there are other compensation cybersecurity controls to have in place; institute an audit trail for at least 5 years; conduct employee training; limit employee access to certain information; and notify the NY DFS Superintendent of breaches (subject to materiality standards).

Joe Thesing from the National Association of Mutual Insurance Companies (NAMIC) stated that the initial version of the NY DFS cybersecurity regulations were very problematic, and while the final version is much improved, the regulations are too prescriptive. One provision that should be included is a carve-out for companies with less than 10 employees. Mr. Thesing stated that NAMIC is not yet in a position to support either the NY DFS regulations or the NAIC Insurance Data Security Model Law (Cyber Model), but that the Cyber Model seems to be heading in the right direction.

Chara Bradstreet of the National Association Insurance Commissioners (NAIC) stated that the NAIC received numerous comments stating that drafting the NAIC Cyber Model based on the NY DFS approach made sense. The NAIC has accordingly narrowed its focus to setting risk-based standards for data security and investigation and notification to the Commissioner of a cybersecurity event. Both the NY DFS regulations and the NAIC Cyber Model delegate notification to consumers to the already existing data notification laws which have been adopted by 48 states. Ms. Bradstreet stated that, regarding the risk-based standards for data security, New York takes a more rules-based approach while the NAIC takes a principles-based

approach. From the beginning, the NAIC has sought to take a more flexible approach, making it easier for smaller licensees to comply. The NAIC has incorporated some of the NY DFS regulation language in its Cyber Model and has made sure that if a licensee complies with the NY DFS regulations, they are deemed to be complaint with the NAIC Cyber Model. Some of the provisions in the current draft of the NAIC Cyber Model that are similar to those in the NY DFS regulations are: using the same definition of non-public information that must be protected; using a similar definition of 'cybersecurity event'; risk-management standards based on the licensee's own risk-assessment; oversight of third party service provider arrangements; requiring an incident response plan; and requiring an annual report to be filed with Commissioner. Ms. Bradstreet further stated that exceptions have been added to the NAIC Cyber Model, including licensees with less than 10 employees; using an information security program of another licensee doesn't need to create its own program. Also, there is an exemption for those licensees compliant with HIPAA data security laws that is not present in the NY DFS regulations.

Larry Eckhouse from the American Insurance Association (AIA) stated that insurers are in the process of implementing the requirements of the NY DFS regulations. IT systems are generally structured in a manner that applies across corporate entities in a system and are not individualized by a state. Thus, it is critical that state data security requirements be harmonized to avoid creating a patchwork of laws that currently exists for data breach notifications – a patchwork will only serve to reduce security rather than enhance it. Mr. Eckhouse stated that there are some challenging components in the NY DFS regulations, but the critical component is that they are risk-based. Using that approach, a company is in the best position to understand which risks it faces and how best to deploy resources to combat such risks. To that extent, states that are looking to implement data security standards should be consistent with the NY DFS regulations and not establish conflicting or additional requirements. The AIA is still reviewing the most recent draft of the NAIC Cyber Model, and noted that it is important to ensure that the definition of a 'cybersecurity event' is tailored in a way that focuses on the materiality of the event and not include an overly broad universe of incidents that have no potential impact on consumers. That is important because a 'cybersecurity event' triggers many of the requirements in the regulations.

Sen. Bob Hackett (OH), Chair of the Committee, asked for information regarding safe harbor provisions. Ms. Bradstreet stated that the NAIC is aware of the concern of companies regarding safe harbor provisions and it is continuing to be discussed. Ms. Filipakis stated, as far as she knows, there are no safe harbor provisions in the NY DFS regulations. Sen. Hackett asked Ms. Filipakis how the NY DFS dealt with the differences between small and large companies. Ms. Filipakis stated that there are carve outs in the NY DFS regulations for licensees with less than 10 employees, and carve outs based on assets and revenue. Sen. Hackett asked whether there are a lot of differences between the NY DFS regulations and the NIST standards. Ms. Filipakis stated that the NY DFS regulations follows a large amount of the NIST standards but an obvious difference is that the NIST standards are voluntary whereas the NY DFS regulations are mandatory.

Rep. Matt Lehman (IN) asked if the less than 10 employee carve out in the NY DFS regulations applied to all types of licensees/entities. Ms. Filipakis stated that she would have to look at the specific language of the regulations to answer that question. Sen. Hackett stated that in Ohio, their cybersecurity task force was assured that the cost of compliance for smaller entities is not as burdensome as previously thought.

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

Sen. Travis Holdman (IN), NCOIL Immediate Past President, stated that the Consumer and Financial Protection Bureau (CFPB) was never needed and that the Resolution seeks to exempt community banks from its onerous and unnecessary regulations. There are trillions of dollars sitting on the sidelines because of fears regarding required capital requirements. In the end, the consumers get hurt because there aren't enough dollars to loan. The fear is that community banks will continue to disappear because the cost of compliance with CFPB regulations is so burdensome. Sen. Hackett noted that in Ohio, the community bank industry has hired more people for regulatory compliance than any other position.

Kevin McKechnie of the American Bankers Association (ABA) stated that in Utah, the Zions Bank compliance staff has doubled since Dodd-Frank was enacted, and one-quarter of the sales staff has been let-go. Additionally, Zions has spent $25 million in consultant services – which is $25 million less available for loans. Mr. McKechnie also stated that between 2000 and 2005, quarterly loan growth was 1.9% - it is half that now. There is also a massive consolidation process happening due to the CFPB's onerous regulations. Mr. McKechnie urged the Committee to write to Congress requesting regulatory relief for community banks.

Julie Gackenbach of Confrere Strategies stated that since the financial crisis, there have been almost 200 new regulations, totaling almost 6,000 pages. Ms. Gackenbach stated that there is a Federal piece of legislation, H.R. 1264 - Community Financial Institution Exemption Act – that has the same goal of Sen. Holdman's Resolution and urged NCOIL to support it.

Sen. Holdman requested that a Motion to adopt his Resolution be accompanied by a request for NCOIL staff to issue a press release announcing its adoption and to send it to all meeting attendees so they can send to their Congressmen and local news outlets. Upon a Motion made and seconded, the Committee unanimously adopted Sen. Holdman's Resolution and press release request.

DISCUSSION ON FINANCIAL CHOICE ACT OF 2017

Mr. McKechnie stated that the CHOICE Act (the Act), among other things, would codify what has already been decided in court – that the CFPB Director is responsible to the President and can accordingly be fired by the President. There are also regulatory relief mechanisms contained in the Act similar to Sen. Holdman's resolution. The Act is pending in the Senate, which is currently working on its own Dodd-Frank reform legislation. Mr. McKechnie stated that the odds are not good for any such legislation being signed into law anytime soon and that the Committee should continue this discussion at the NCOIL Annual Meeting in November. Mr. McKechnie also noted that, unfortunately, relief from the Durbin Amendment was not put in the Act.

Frank O'Brien from the Property Casualty Insurance Association of America (PCIAA) stated that the politics surrounding the Act have not matched up with the aspirations of Dodd-Frank reform. There is widespread acknowledgement in both parties that Dodd-Frank needs to be tweaked, but there is also acknowledgement that it appears unlikely anytime soon. Mr. O'Brien stated that NCOIL, as defenders and communicators of the state-based system of insurance regulation, has an important role to play as the debate continues, and urged NCOIL to continue to stay involved.

Ms. Bradstreet stated that the NAIC believes that the Act has promise but improvements need to be made to ensure that it works for the insurance sector and its regulation. One concern is the inclusion of the Office of the Independent Insurance Advocate – a policy office with its proposed size, scope, independence, and rulemaking authority within the Treasury Department would be unprecedented and would create an entity with the trappings of a regulator. The office assumes, with some minor modifications, FIO's authorities and NAIC believes that a standalone office is not needed to carry out such authorities. The roles for which FIO or an independent insurance advocate could provide some value, such as running the Terrorism Risk Insurance program, could be filled by the Treasury Department.

Ms. Bradstreet stated that the NAIC agrees that the non-bank designation process is in need of significant reform and is pleased that the Act seeks to address those concerns that the NAIC and others have with an arbitrary process that has yielded procedurally and substantively flawed designations of insurance firms. Lastly, Ms. Bradstreet stated that to ensure that the insurance perspective is adequately represented in FSOC discussions, state insurance regulators should be given voting authority.

Rep. George Keiser (ND) stated that when Dodd-Frank was enacted there was at least one area where states had an option: the selling and sharing of personal information. North Dakota was the only state to reverse that provision in Dodd-Frank. Rep. Keiser asked if there was any other similar flexibility contained within Dodd-Frank. Mr. McKechnie stated that it is his understanding that there is not.

ADJOURNMENT

There being no further business, the Committee adjourned at 11:15 a.m.