NATIONAL COUNCIL OF INSURANCE LEGISLATORS
FINANCIAL SERVICES COMMITTEE
OKLAHOMA CITY, OKLAHOMA
DECEMBER 6, 2018
DRAFT MINUTES

The National Council of Insurance Legislators (NCOIL) Financial Services Committee met at The Renaissance Oklahoma City Convention Center Hotel in Oklahoma City, Oklahoma on Thursday, December 6, 2018 at 2:15 p.m.

Representative Sam Kito of Alaska, Vice Chair of the Committee, presided.

Other members of the Committees present were:

Asm. Ken Cooley (CA)
Rep. Martin Carbaugh (IN)
Rep. Matt Lehman (IN)
Rep. Joseph Fischer (KY)
Rep. Steve Riggs (KY)
Rep. Edmond Jordan (LA)
Sen. Dan "Blade" Morrish (LA)
Rep. George Keiser (ND)
Sen. Jerry Klein (ND)
Asm. Andrew Garbarino (NY)
Asw. Pamela Hunter (NY)
Rep. Tom Oliverson, M.D. (TX)

Other legislators present were:

Sen. Gary Dahms (MN)
Sen. Paul Utke (MN)
Rep. Joe Schmick (WA)

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

A motion was first made by Rep. Tom Oliverson, M.D. (TX) and seconded by Sen. Jerry Klein (ND) to waive the quorum requirement which the Committee approved without objection by way of a voice vote. Upon a motion made by Asm. Ken Cooley (CA) and seconded by Rep. Joseph Fischer (KY), the Committee approved without objection by way of a voice vote the minutes of its July 13, 2018 meeting in Salt Lake City, UT.

UPDATE ON DATA SECURITY AND BREACH NOTIFICATION LAWS

Paul Ferrillo of GreenbergTraurig, LLP, stated that the current state of cybersecurity is not good, particularly with the very recent news regarding the Marriott and Quora breaches. The only way things are going to get better is by continuing the dialogue surrounding cybersecurity. In the past month alone, there have probably been approximately one billion records hacked or stolen. Mr. Ferrillo stated that he worked on some of the big third party vendor media hacks in addition to several others. Legislation is not working well because whenever we have a piece of legislation introduced it seems like it takes six or seven years to actually sign it into law.

One big issue on almost everyone's mind is the national data breach notification rule. For those in the different industries and different states, there are several different rules and guidelines that must be met relating to breach notification requirements. Some people are talking about whether or not there should be federal guidance that preempts state laws. An example of that is H.R. 6743 – The Consumer Information Notification Requirement Act – sponsored by Congressmen Luetkemeyer. Mr. Ferrillo stated that in his opinion, none of it really matters. Whether you must report a breach in one day or 72 hours is not going to matter.

Mr. Ferrillo stated that he spent on behalf of one client easily $20,000 in attorney time giving notifications of a huge data breach to all 50 states and 37 countries. Something does not make much sense when you are talking about that much money being spent when millions of pieces of personally identifiable information (PII) had already been obtained. Mr. Ferrillo stated that, in the spirit of a conversation held earlier during which the National Association of Insurance Commissioners (NAIC) was the focus, something that would go against the NAIC's wishes would be if states adopted the NIST Cybersecurity Framework, which is actually Federal guidance but a common sense framework that you may or may not know has been incorporated in many different state regimes and federal laws, in addition to the new General Data Protection Regulation (GDPR) in the EU if you look "under the hood" of that regulation.

Mr. Ferrillo stated that the NIST framework is a document that will get the U.S. "out of jail" and "out of the doghouse." Mr. Ferrillo urged the legislators present to adopt the NIST framework in each of their states because you can have any genius stand up and tell you what is wrong with the state of cybersecurity and they will all be wrong. They can be right by adopting the NIST framework. With regard to incident responses, Mr. Ferrillo stated that they are a big problem. You must report an incident affecting consumers of a particular magnitude and the magnitude differs from state to state and the reporting requirements also differ depending on the type of information obtained in the incident. Mr. Ferrillo stated that the big problem with cybersecurity today is that no one is talking about how to fix something; everyone is talking about remedial actions.

Mr. Ferrillo stated that one of the biggest problems today related to cybersecurity is also aging infrastructure. You cannot run a state or a business effectively using Windows XP or Windows 7. Software needs to be updated but paying for it is of course an issue. There will be no end in cybersecurity attacks unless we all take the bull by the horns and do something that actually makes sense. We will not be able to sustain this country when we're dealing with 47 parts of the U.S. government that are unconnected to each other and not protected by the NSA or other large government body.

Justin Brookman, Director of Consumer Privacy and Technology at ConsumersUnion, stated that, just like the current state of cybersecurity, the current state of data privacy is also not good at all. The recent news of Facebook accessing consumer's call logs without notice in order to suggest friends affirms that statement. Mr. Brookman stated that U.S. law on privacy is a relatively new concept and has evolved slowly since Justice Brandeis raised concerns in 1890. Sectoral specific laws have emerged, which have done a good job of protecting types of data, such as the Fair Credit Reporting Act (FCRA); Children's Online Privacy Protection Act (COPPA); Health Information Portability and Accountability Act (HIPAA); and the Video Privacy Protection Act (VPPA). However, a lot of your personal information is not well protected.

Mr. Brookman stated that many of the aforementioned laws look somewhat similar and have similar principles based on the Fair Information Practice Principles. The problem is that most data is not covered by those laws which is unusual because most countries around the world have basic privacy protections for all information. Since 1995, Europe has had such legislation and the EU also just passed the GDPR, designed to be a more rigorous version of their existing law. Mr. Brookman stated that in the U.S., the Federal Trade Commission (FTC) is the default privacy regulator but they don't have a privacy law, but rather broad prohibitions on "deceptive" and "unfair" business practices set forth in Section 5 of the FTC Act. "Deception" is a good standard, but the Act doesn't say much beyond "don't lie" which means privacy policies tend to be very vague. It is also unclear as to what is "unfair" in the privacy space since the Act was not really designed to address the privacy issues we deal with today.

Mr. Brookman stated that states have historically taken the lead on privacy and security issues. States have constitutional protections surrounding personal information. New Hampshire recently passed a ballot initiative to approve an amendment to the state's constitution: "An individual's right to live free from governmental intrusion in private or personal information is natural, essential, and inherent." The federal government still has not caught up with states regarding breach notification laws and almost half the states have data security laws.

Mr. Brookman stated that the recently passed California Consumer Privacy Act of 2018 (CCPA) is the most sweeping and ambitious privacy law passed in the U.S. The CCPA came about very suddenly in that a real estate developer, Alastair MacTaggart, started having conversations with his friends from Silicon Valley and realized that a comprehensive privacy law was needed due to their complex activities. Mr. MacTaggart then sponsored a ballot initiative and was not sure if it was going to advance but then the Facebook-Cambridge Analytica story broke and that spurred the initiative forward. California legislators thought that ballot initiatives were not the best way to make laws dealing with data security and technology, so they worked out a deal whereby the legislature would pass a law that could be amended more easily if Mr. MacTaggart dropped the ballot initiative.

The entire process went very quickly and the CCPA reads as such as there are many inconsistencies. Some amendments have already been introduced in an effort to clean it up, but the process is nowhere near finished. The CCPA applies to all entities doing business in California that make more than $25 million in annual revenue, have personal data on 50,000 or more people, or data brokers, which is what the Act was really designed to "get to" – data brokers who get information about you and sell that information. It is unclear whether the CCPA applies to non-profits but it is clear that it covers a very broad amount of information: essentially any information that could relate to you.

Mr. Brookman stated that the CCPA adds four new rights for individuals: transparency; access to data; opt-out of sharing; and deletion. Regarding transparency, privacy policies don't really say much today. Some states require privacy policies, but the laws don't really state what the policy must contain. Accordingly, the CCPA tries to set forth what must be in privacy policies. Regarding access to data, the CCPA permits a consumer, twice per year, to request specific pieces of information from any covered business. That is certainly a feature of European privacy laws. Regarding opting-out of sharing information, if you go to the grocery store and they generated a profile of all of

the groceries you bought, you can tell them to not sell it to data brokers. There are important exceptions to that right, notably for sharing limited information for "business purposes" to service providers, but it nonetheless is a very broad right. However, it is not clear how that right will apply to online advertisement (and other third-party) tracking and that is an issue that may be addressed through amendments. Regarding deletion, you can direct a company to delete any data it has about you, with certain exceptions.

Mr. Brookman stated that the CCPA prohibits the selling of information about minors under 16 years of age without affirmative consent from the parent or minor, depending on the age of the minor. One of the controversial parts of the CCPA deals with whether a company can charge an individual more or offer lower quality to someone who exercises their privacy rights and opts out of sharing their information. Mr. Brookman stated that he understands the arguments on both sides of that issue. The language in the ballot initiative prohibited companies from doing so but the language that passed states that the company can offer the individual an incentive to allow them to sell your information or they can charge the individual more if it reasonably relates to the value that the data provides. No one is quite sure what that means.

Regarding enforcement, Mr. Bookman stated that the CCPA provides for a penalty of up to $7,500 per violation which can be incredibly onerous particularly for companies like Facebook that has billions of users. The enforcement provisions were somewhat watered down in the final version. There was a whistleblower provision, municipality enforcement provisions, and provisions providing for a private cause of action but those are all by and large removed from the statute as enacted. In 2019, the CA Attorney General will be promulgating regulations to clarify certain outstanding issues such as who exactly is covered under the CCPA, how do you obtain verifiable consent from an individual and how do you make the opt-out provisions work at scale.

Mr. Brookman stated that in some ways the CCPA does not address all the concerns raised by privacy advocates as the focus is more on small data brokers rather than large companies like Google and Facebook. Some privacy advocates have called for provisions that require companies to only collect the data that they need, and that require companies to obtain permission for certain things rather than putting the burden on the user to tell the company to stop collecting and selling data. Nevertheless, Mr. Brookman stated that the CCPA is a significant advancement in privacy protections. The CCPA probably will not get repealed, but a big fight is in store for those in California in 2019 as amendments are expected to be considered and litigation is underway with plaintiffs raising concerns related to the Commerce Clause and the 1st Amendment, among others.

Mr. Brookman stated that with regard to security legislation, about half of the states have such legislation that states if you have information, reasonable procedures need to be in place to ensure it is not stolen. The legislation is roughly consistent with authority the FTC has asserted under its Unfair, Deceptive or Abusive Acts and Practices (UDAP) authority. One new development in California last year was the enactment of cybersecurity legislation which does not deal with information security but rather with protecting certain things such as "smart" washing machines so that they cannot be hacked and manipulated. Mr. Brookman further stated that there is also a tremendous amount of interest in these issues at the federal level but he is not optimistic of seeing anything passed anytime soon.

Michael Gugig, Vice President of State Gov't Relations & Assoc. General Counsel at Transamerica began by sating that his remarks today are on behalf of the American Council of Life Insurers (ACLI). Mr. Gugig stated that there is a fundamental need to secure policyholder information. Life insurers have a long history of dealing with highly sensitive personal information from their customers. Much of that is medical information, which life insurers need. Without that information, underwriting cannot occur and claims cannot be paid because life insurers need to be able to get the information both at the start of the sales process and when it comes time to pay the claim. Life insurers are acutely aware of the type of data that they have and the need to secure it.

Mr. Gugig stated that life insurers have been strong supporters of carefully thought through state and federal laws that together comprise a broad and rigorous regulatory framework that requires life insurers to protect both the privacy and security of customer information. Mr. Gugig then discussed some differences between security and privacy laws. Security laws and regulations tell us how our systems have to be protected so that hackers cannot steal information. Privacy laws and regulations tell us what companies can do with the information once they have it. The CCPA is an example of a privacy law. Many people conflate those two types of laws but it is important to recognize the differences.

Mr. Gugig stated that virtually every state has multiple laws in place that govern how insurers, particularly life insurers, are required to safeguard customer information. With regard to the CCPA, it is important to note that insurers are in a unique position because they need certain information from customers; insurers are not just gathering information so that they can sell it to others. Insurers are gathering information in order to conduct the business of insurance. The CCPA was passed in a very short period of time and was literally in the legislature for only a few days. There was a lot of brokering behind closed doors and no consideration as to how the law might affect regulated industries like the insurance business as there are already multiple CA laws and regulations that insurers must comply with. Accordingly, when laws like the CCPA are passed without thoughtful consideration of how it might affect certain industries, the impact can be profound. Mr. Gugig also noted that there are federal laws in place that insurers must comply with such as Gramm-Leach-Bliley, the Fair Credit Reporting Act, and HIPAA.

Mr. Gugig further stated that the main point is that the life insurance industry believes fundamentally in the need for uniformity and harmonization. Think for a moment of the difficulty that a 50-state business encounters when having to utilize computer systems and secure them in 50 different ways subject to different laws and regulations within each state. It also becomes extraordinarily difficult to know which law and rule is working and which ones are not working because some of the laws and rules have been enacted without enough consultation as to how some unintended consequences might arise. Insurers generally keep data on systems on a national level, not on a state-by-state basis. In the absence of a uniform privacy and data security protocol, insurers that conduct business across the country end up defaulting to the most draconian standard because in theory they will then by complying with all laws. By forcing the industry to act in such a manner, public policy agendas will not be satisfied.

Going back to the CCPA, Mr. Gugig stated that it is a generally applicable law. Without thoughtful consideration of how it will impact all covered entities, it is going to be extraordinarily difficult for there to be an understandable comprehensive data security and data privacy system. The complexity of the current regulatory structure and new

and growing privacy and security challenges make careful and thoughtful consideration necessary regarding the need for and substance of any new privacy or security law applicable to life insurers. We need to be thinking about these issues on an industry-by-industry analysis. The hope is that insurers will not be subject to any more breaches, but the fear is that they might be, and without a uniform system of data security and data privacy, the likelihood of breaches will grow.

Rep. Sam Kito (AK) – Vice Chair of the Committee – stated that with regard to the problem of regulating these issues state-by-state, are there any industries and organizations seeking to enact a national standard? Mr. Gugig stated that there is an appetite in Congress for federal preemptive legislation. The life insurance industry strongly supports state regulation of insurance and wants there to be uniformity between the states and wants state insurance regulators to regulate how insurers protect consumer's data as opposed to Attorneys General. The fear is that if that does not prove to be workable, a federal standard will be enacted.

Asm. Ken Cooley (CA) – NCOIL Secretary – noted that the basic path of the CCPA was a ballot initiative which means the drafters of the law "did their own thing" and it was exceedingly stringent and on the November ballot. A facet of CA law is that if you qualify something to go on the ballot, if the legislature passes something similar that the mover of the initiative is agreeable to, the legislation can be passed and the initiative can be pulled. Accordingly, a bill was then drafted quickly as an alternative to the more stringent ballot version and the legislature now has until January 1, 2020, to implement the bill.

DISCUSSION/CONSIDERATION OF RESOLUTION IN SUPPORT OF STATE REGULATED HEALTH SAVINGS ACCOUNT-BASED COVERAGE

Rep. Steve Riggs (KY) – NCOIL Immediate Past President – provided some background on a proposed "Resolution in Support of State Regulated Health Savings Account-Based Coverage" which he and Sen. Jerry Klein (ND) co-sponsored for consideration. Health savings accounts (HSAs) have become the fastest growing product in the insurance market. The Resolution aims to inform states to essentially avoid the actions that certain states such as Illinois, Maryland, Oregon, and Vermont undertook relating to enacting laws requiring fully-insured plans issued within their borders to cover male sterilization benefits without application of the plan deductible, copays or coinsurance. Those laws effectively made HSAs inoperable in those states because the laws go beyond a clear understanding of what the IRS considers "preventive care services" that could be exempt from the deductible. HSAs are linked to high deductible health plans (HDHPs), which must meet certain requirements, most notably that the plan deductible must apply to all covered benefits received from in-network providers – the only exception being for "preventive care services" as defined by the IRS.

Sen. Klein stated that the Resolution is an important step in making sure those with HSAs are able to continue making contributions to such accounts. Sen. Klein stated that he discussed the Resolution with ND Insurance Cmsr, Jon Godfread, who supported it.

Kevin McKechnie of the American Bankers Association (ABA) stated that the issue the Resolution deals with is very easy to understand. HSAs and qualified insurance are defined under IRS code but in the individual, fully-insured market, HSA-qualified insurance is insurance that adheres to IRS code and the many rules of each state.

Accordingly, when those two qualifiers conflict, everyone in the conflicting state with an HSA becomes ineligible to contribute to their HSA and must find replacement coverage. The Resolution therefore is in support of states respecting federal IRS code and when a state chooses to enact a mandate, there is no issue with what the mandate is, people who have HSA-qualified insurance can keep that coverage. More specifically, the Resolution encourages to follow the path of what Vermont did which was to adopt language that exempts HSA-qualified insurance from having to meet a certain first-dollar coverage requirement.

Upon a Motion made by Rep. Riggs and seconded by Sen. Klein, the Committee voted without opposition to adopt the Resolution as amended by way of a voice vote. The amendment served to add to the list of recipients that the Resolution directs NCOIL staff to send to.

DISCUSSION/CONSIDERATION OF RESOLUTION ASSERTING MCCARRAN-FERGUSON REVERSE PREEMPTION OVER THE SUPERVISION OF INSURANCE COMPANIES BY THE FEDERAL RESERVE BOARD AND ITS EXAMINERS

Paul Martin, Regional Vice President, Southwestern Region, of the National Association of Mutual Insurance Companies (NAMIC) spoke in support of a Resolution "Asserting McCarran-Ferguson Reverse Preemption over the Supervision of Insurance Companies by the Federal Reserve Board and its Examiners", sponsored by Sen. Dan "Blade" Morrish (LA) – NCOIL Vice President.

Mr. Martin stated that the McCarran-Ferguson Act was passed by Congress in 1945 in response to a U.S. Supreme Court decision that held that insurance was commerce and therefore should be regulated by Congress. The McCarran-Ferguson Act has allowed insurance companies and consumers to greatly benefit. Insurance companies are allowed to, in a very limited sense, share information and work together on forms and create different types of products that are available and affordable for consumers. This process has worked well for the marketplace, however, there has recently been some incremental encroachment by the Federal Reserve by seeking and asking for information that is already being regulated by state regulators. Mr. Martin stated that NAMIC feels very passionately that state regulation is the best option for the insurance industry. The Resolution is necessary to send a message to Congress and the Federal Reserve that current Federal law puts state regulation of insurance at the forefront.

Sen. Morrish pointed to the Resolution's penultimate paragraph which states that the actions which the Resolution calls for are not only consistent with the McCarran-Ferguson Act, but with the Gramm-Leach-Bliley Act, and the Dodd-Frank Act. The Federal Reserve should stay out of state regulated insurance operations, regardless of the insurer's affiliations with federally-regulated financial institutions.

Upon a Motion made by Sen. Morrish and seconded by Sen. Klein, the Committee voted without opposition to adopt the Resolution by way of a voice vote.

ADJOURNMENT

There being no further business, the Committee adjourned at 3:30 p.m.