Testimony of

Adam W. Hamm

Commissioner

North Dakota Department of Insurance

On Behalf of the National Association of Insurance Commissioners

Before the

Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies

Committee on Homeland Security

United States House of Representatives

Regarding:

The Role of Cyber Insurance in Risk Management

March 22, 2016

Introduction

Chairman Ratcliffe, Ranking Member Richmond, and members of the Subcommittee, thank you for the invitation to testify today. My name is Adam Hamm. I am the Commissioner of the Insurance Department for the state of North Dakota and I present today's testimony on behalf of the National Association of Insurance Commissioners (NAIC).[1] I am a Past President of the NAIC, and I have served as the Chair of the NAIC's Cybersecurity Task Force since its formation in 2014.[2] On behalf of my fellow state insurance regulators, I appreciate the opportunity to offer our views and perspective on cybersecurity challenges facing our nation and the role cybersecurity insurance can play in risk management.

The Cyber Threat Landscape Creates Demand for Coverage

On one hand, threats to data privacy are not new for businesses, regulators, or the consumers we protect. Regulators and legislatures have required businesses to protect consumer data for decades. On the other hand, the modern size, scale, and methods of data collection, transmission, and storage all present new challenges. As society becomes more reliant on electronic communication and businesses collect and maintain ever more granular information about their customers in an effort to serve them better, the opportunity for bad actors to inflict damage on businesses and the public increases exponentially. Rather than walking into a bank, demanding bags of cash from a teller, and planning a speedy getaway, a modern thief can steal highly sensitive personal health and financial data with a few quick keystrokes or a well disguised phishing attack from the comfort of his basement couch. Nation states also place great value on acquiring data to either better understand or disrupt U.S. markets, and are dedicating tremendous resources to such efforts.

As these cyber threats continue to evolve, they will invariably affect consumers in all states and territories. State insurance regulators are keenly aware of the potential devastating effects cyber-attacks can have on businesses and consumers, and we have taken a number of steps to enhance data security expectations across the insurance sector, including at our own departments of insurance and at the NAIC. We also understand the pressure these increased risks are putting on other industries, creating unprecedented demand for products that allow purchasers to manage and mitigate some of their cybersecurity risks through insurance. Whether attacks come from nation states, terrorists, criminals, hacktivists, external opportunists or company insiders, with each announcement of a system failure leading to a significant business loss, awareness grows, and companies will seek additional coverage for security breaches, business interruptions,

---

[1] The NAIC is the United States standard-setting and regulatory support organization created and governed by the chief insurance regulators from the 50 states, the District of Columbia, and five U.S. territories. Through the NAIC, we establish standards and best practices, conduct peer review, and coordinate our regulatory oversight. NAIC members, together with the central resources of the NAIC, form the national system of state-based insurance regulation in the U.S.

[2] Attachment A – NAIC Cybersecurity (EX) Task Force Membership List

reputational damage, theft of digital assets, customer notifications, regulatory compliance costs, and many more liabilities that arise from doing business in the modern connected universe.

Most businesses carry and are familiar with their commercial insurance policies providing general liability coverage to protect the business from injury or property damage. What they may not realize is that most standard commercial lines policies do not cover many of the cyber risks mentioned above. To cover these unique cyber risks through insurance, businesses need to purchase a special cybersecurity policy.

I want to urge some caution regarding the term "cybersecurity policy" because it can mean so many different things – while it is a useful short-hand for purposes of today's conversation, I want to remind the Committee that until we see more standardization in the marketplace, a "cybersecurity policy" will really be defined by what triggers the particular policy and what types of coverage may or may not be included depending on the purchaser and insurer. Commercial insurance policies are contracts between two or more parties, subject to a certain amount of customization, so if you've seen one cybersecurity policy, you've seen exactly one cybersecurity policy.

All these nuances mean securing a cybersecurity policy is not as simple as pulling something off the shelf and walking to the cash register. Insurers writing this coverage are justifiably interested in the risk-management techniques applied by the policyholder to protect its network and its assets. The more an insurer knows about a business's operations, structures, risks, history of cyber-attacks, and security culture, the better it will be able to design a product that meets the client's need and satisfies regulators.

Insurance Regulation in the U.S. – "Cops on the Beat"

The U.S. insurance industry has been well-regulated at the state level for nearly 150 years. Every state has an insurance commissioner responsible for regulating that state's insurance market, and commissioners have been coming together to coordinate and streamline their activities through the NAIC since 1871. The North Dakota Insurance Department, which I lead, was established in 1889 and employs approximately 50 full-time staff members to serve policyholders across our state. It is our job to license companies and agents that sell products in our state, as well as to enforce the state insurance code with the primary mission of ensuring solvency and protecting policyholders, claimants, and beneficiaries, while also fostering an effective and efficient marketplace for insurance products. The strength of our state-based system became especially evident during the financial crisis – while hundreds of banks failed and people were forced from their homes, less than 20 insurers became insolvent and even then, policyholders were paid when their claims came due.

Conceptually, insurance regulation in the United States is straightforward. Americans expect insurers to be financially solvent, and thus able to make good on the promises they have made. Americans also want insurers who treat policyholders and claimants fairly, paying claims when they come due. In practice, the regulation of an increasingly complex insurance industry facing constantly changing risks and developing new products to meet risk-transfer demand becomes challenging very quickly. The U.S. state-based insurance regulatory system is unique in that it

relies on an extensive system of peer review, communication, and collaboration to produce checks and balances in our regulatory oversight of the market. This, in combination with our risk-focused approach to financial and market conduct regulation, forms the foundation of our system for all insurance products in the U.S., including the cybersecurity products we are here to discuss today.

Treasury Deputy Secretary Sarah Bloom Raskin stated at an NAIC/CSIS event last fall that "state insurance regulators are the cops on the beat when it comes to cybersecurity at insurance companies and the protection of sensitive information of applicants and policyholders." We take very seriously our responsibility to ensure the entities we regulate are both adequately protecting customer data and properly underwriting the products they sell, and we continue to convey the message to insurance company C-suites that cybersecurity is not an IT issue – it is an Enterprise Risk Management Issue, a Board of Directors issue, and ultimately a CEO issue.

Regulation of Cybersecurity Policies

Having discussed increasing demand for coverage, we can turn to the role my fellow insurance commissioners and I play as regulators of the product and its carriers. Let me start by putting you at ease: when it comes to regulation, cybersecurity policies are scrutinized just as rigorously as other insurance contracts. While they may be more complex than many existing coverages and new product language will present some novel issues, when insurers draft a cybersecurity policy, they are still required to file forms and rates subject to review by the state Department of Insurance. State insurance regulators review the language in the contracts to ensure they are reasonable and not contrary to state laws. We also review the pricing and evaluate the benefits we expect to find in such policies. State regulators also retain market conduct authorities with respect to examinations of these insurers and policies in order to protect policyholders by taking enforcement measures against bad actors.

Insurance regulation involves front-end, ongoing, and back-end monitoring of insurers, products, and insurance agents (or producers). The system's fundamental tenet is to protect policyholders by ensuring the solvency of the insurer and its ability to pay claims. Strict standards and keen financial oversight are critical components of our solvency framework. State regulators review insurers' material transactions for approval, restrict key activities, have explicit financial requirements, and monitor compliance and financial condition through various solvency surveillance and examination mechanisms, some of which we recently updated to incorporate cybersecurity controls. We can also take corrective action on insurers when necessary through a regulatory intervention process.

Financial Regulation

Financial regulation is focused on preventing, detecting, and resolving potentially troubled insurers. Insurance regulators carefully monitor insurers' capital, surplus, and transactions on an ongoing basis through financial analysis, reporting requirements, actuarial opinions, and cash

flow testing. State insurance laws also restrict insurers' investments and impose capital and reserving requirements.

The monitoring of insurers is done through both on-site examinations and analysis of detailed periodic insurer reporting and disclosures. Insurers are required to prepare comprehensive financial statements using the NAIC's Statutory Accounting Principles (SAP). SAP utilizes the framework established by Generally Accepted Accounting Principles (GAAP), but unlike GAAP which is primarily designed to provide key information to investors of public companies and uses a going-concern concept, SAP is specifically designed to assist regulators in monitoring the solvency of an insurer. The NAIC's *Accounting Practices and Procedures Manual* includes the entire codification of SAP and serves as the consistent baseline accounting requirement for all states. Each insurer's statutory financial statements are filed with the NAIC on a quarterly and annual basis and include a balance sheet, an income statement, and numerous required schedules and exhibits of additional detailed information.

The NAIC serves as the central repository for an insurer's financial statement data, including running automated prioritization indicators and sophisticated analysis techniques enabling regulators around the country to have access to national-level data without the redundancy of reproducing this resource in every state. This centralized data and analysis capability has been cited by the IMF as world leading.

Cybersecurity risk remains difficult for insurance underwriters to quantify due in large part to a lack of actuarial data. This has potential implications for ongoing regulation and the market for the product. If a product is priced too low, the insurer may not have the financial means to pay claims to the policyholder. If too high, few businesses and consumers can afford to purchase it, instead opting to effectively self-insure for cyber incidents, limiting the ability of the insurance sector to be used as a driver of best practices. Today, in the absence of such data, insurers compensate by pricing that relies on qualitative assessments of an applicant's risk management procedures and risk culture. As a result, policies for cyber risk tend to be more customized than policies for other risks, and, therefore, more costly. The type of business operation seeking coverage, the size and scope of operations, the number of customers, the presence on the web, the type of data collected, and how the data is stored will all be among the factors that dictate the scope and cost of cybersecurity coverage offered. From a regulatory perspective, though, we would like to see insurers couple these qualitative assessments with robust actuarial data based on actual incident experience.

Prior to writing the policy, the insurer will want to see the business' disaster response plan and evaluate it with respect to network risk management, websites, physical assets, intellectual property, and possibly even relationships with third-party vendors. The insurer will be keenly interested in how employees, contractors, and customers are able to access data systems, how they are trained, and who key data owners are. At a minimum, the insurer will want to know about the types of antivirus and anti-malware software the business is using, the frequency of system and software updates performed by the business, and the performance of the firewalls the business is using.

Examination Protocols and Recent Updates

Last year, the NAIC, through a joint project of the Cybersecurity Task Force and the IT Examination Working Group, undertook a complete review and update of existing IT examination standards for insurers. Prior to this year, regulatory reviews of an insurer's information technology involved a six step process for evaluating security controls under the COBIT 5 framework. Revisions for 2016 to further enhance examinations are based in part on the NIST framework "set of activities" to Identify, Protect, Detect, Respond, and Recover. Specific enhancements were made to the NAIC *Financial Examiner's Handbook* regarding reviews of insurer cybersecurity training and education programs, incident response plans, understanding cybersecurity roles and responsibilities, post-remediation analyses, consideration of third party vendors, and how cybersecurity efforts are communicated to the Board of Directors.

Also evolving are regulators' expectations of insurance company C-suites – specifically Chief Risk Officers and Boards of Directors. Regulators expect improved incident response practice exercises, training, communication of cyber risks between the board and management, and incorporation of cyber security into the Enterprise Risk Management processes. There is now an expectation that members of an insurer's board of directors will be able to describe how the company monitors, assesses, and responds to information security risks.

Market Regulation

Market regulation is focused on legal and fair treatment of consumers by regulation of product rates, policy forms, marketing, underwriting, settlement, and producer licensing. Market conduct examinations occur on a routine basis, but also can be triggered by complaints against an insurer. These exams review producer licensing issues, complaints, types of products sold by insurers and producers, producer sales practices, compliance with filed rating plans, claims handling and other market-related aspects of an insurer's operation. When violations are found, the insurance department makes recommendations to improve the insurer's operations and to bring the company into compliance with state law. In addition, an insurer or insurance producer may be subject to civil penalties or license suspension or revocation. To the extent that we see any of these issues arising from claims made on cybersecurity policies, regulators will be able to address them promptly through our suite of market conduct tools, and enhancements made to the *Financial Examiner's Handbook* are expected to be incorporated into the *Market Conduct Examiner's Handbook* this year.

Surplus Lines

It is worth mentioning that some cybersecurity coverage is currently being written in the surplus lines markets. A surplus lines policy can be issued only in cases where the coverage cannot be found in traditional insurance markets because the coverage is unique or otherwise difficult to underwrite. Surplus lines insurers that are domiciled in a U.S. state are regulated by their state of domicile for financial solvency and market conduct. Surplus lines insurers domiciled outside

the U.S. may apply for inclusion in the NAIC's Quarterly Listing of Alien Insurers. The carriers listed on the NAIC Quarterly Listing of Alien Insurers are subject to capital and surplus requirements, a requirement to maintain U.S. trust accounts, and character, trustworthiness and integrity requirements.

In addition, the insurance regulator of the state where the policyholder resides (the home state of the insured) has authority over the placement of the insurance by a surplus lines broker and enforces the requirements relating to the eligibility of the surplus lines carrier to write policies in that state. The insurance regulator can also potentially sanction the surplus lines broker, revoke their license, and hold them liable for the full amount of the policy.

Like any other insurance market, as the cybersecurity market grows and more companies offer coverage, we anticipate the regulation will continue to evolve to meet the size and breadth of the market as well as the needs of consumers. State insurance regulators have a long history of carefully monitoring the emergence and innovation of new products and coverages, and tailoring regulation over time to ensure consumers are appropriately protected and policies are available.

Cybersecurity Insurance Market – New Reporting Requirements

As a still nascent market for coverage, accurately assessing exposure or the size of the cybersecurity insurance market is a work in progress. To date, the only analyses of the cybersecurity market come from industry surveys and estimates that consistently place the size of the market in the neighborhood of two to three billion dollars. In light of the uncertainty and many questions surrounding these products and the market, the NAIC developed the new *Cybersecurity and Identify Theft Coverage Supplement*[3] for insurer financial statements to gather financial performance information about insurers writing cybersecurity coverage nationwide.

This mandatory new data supplement, to be attached to insurers' annual financial reports, requires that all insurance carriers writing either identity theft insurance or cybersecurity insurance report to the NAIC on their claims, premiums, losses, expenses, and in-force policies in these areas. The supplement requires separate reporting of both standalone policies and those that are part of a package policy. With this data, regulators will be able to more definitively report on the size of the market, and identify trends that will inform whether more tailored regulation is necessary. We will gladly submit a follow-up report to the Committee once we have received and analyzed the first batch of company filings, which are due April 1, and will keep all stakeholders apprised as we receive additional information. As with any new reporting requirement, we expect the terminology and reporting to mature over time as carriers better understand the specific information regulators need.

Having this data will enable regulators to better understand the existing cybersecurity market, and also help us know what to look for as the market continues to grow, particularly as we see small and mid-size carriers potentially writing these complex products.

---

[3] Attachment B.

NAIC Efforts Beyond Cybersecurity Insurance

The NAIC and state insurance regulators are also ramping up our efforts to tackle cybersecurity issues in the insurance sector well beyond cybersecurity insurance. We understand that the insurance industry is a particularly attractive target for hackers given the kind of data insurers and producers hold, and to that end we are engaged on a number of initiatives to reduce these risks.

The NAIC adopted twelve *Principles for Effective Cybersecurity: Insurance Regulatory Guidance* in April 2015.[4] The principles set forth the framework through which regulators will evaluate efforts by insurers, producers, and other regulated entities to protect consumer information entrusted to them.

We also adopted an NAIC *Roadmap for Consumer Cybersecurity Protections* in December 2015 to describe protections the NAIC believes consumers should be entitled to from insurance companies and agents when these entities collect, maintain, and use personal information and to guide our ongoing efforts in developing formal regulatory guidance for insurance sector participants.[5]

Most recently, on March 3rd, the Cybersecurity Task Force exposed its new *Insurance Data Security Model Law* for public comment – written comments should be submitted by Wednesday, March 23rd, and feedback will be discussed at the open meeting of the task force on April 4th in New Orleans.[6] The purpose and intent of the model law is to establish the exclusive standards for data security, investigation, and notification of a breach applicable to insurance licensees. It lays out definitions and expectations for insurance information security, breach response, and the role of the regulator. Recognizing that one-size does not fit all, the model specifically allows for licensees to tailor their information security programs depending on the size, complexity, nature and scope of activities, and sensitivity of consumer information to be protected. Perhaps most importantly, the model is intended to create certainty and predictability for insurance consumers and licensees as they plan, protect information, and respond in the difficult time immediately following a breach. We welcome all stakeholders' input as we continue the model's development through the open and transparent NAIC process.

Related to the NAIC's new model, we are aware Congress is considering a number of Federal Data Breach bills. While Congress held its first hearings on data breaches 20 years ago, there has been no successful legislation on the issue. Meanwhile, 47 states have acted to varying degrees, and some are on the fourth iteration of data security and breach notification laws. Some of these bills, including S.961/HR 2205, the Data Security Act, would lessen existing consumer

---

[4] Attachment C.

[5] Attachment D.

[6] Attachment E.

protections in the insurance sector and could undermine our ongoing and future efforts to respond to this very serious issue.

Coordinating with our Federal Colleagues

Lastly, we understand that state insurance regulators are not alone in any of our efforts. We work collaboratively with other financial regulators, Congress, and the Administration to identify specific threats and develop strategies to protect the U.S. financial infrastructure. State insurance regulators and NAIC staff are active members of the Treasury Department's Financial Banking and Information Infrastructure Committee (FBIIC), where I recently gave a presentation on insurance regulators' efforts in this space.

We are also members of the Cybersecurity Forum for Independent and Executive Branch Regulators, where we meet with White House officials and other regulators to discuss best practices and common regulatory approaches to cybersecurity challenges across very different sectors of the U.S. economy. While we certainly do not have all the answers yet, rest assured that regulators are communicating and collectively focused on improving cyber security posture across our sectors.

Current State of Play

I recently met with a group of insurance CEO's to discuss the NAIC's ongoing efforts in data and cybersecurity. Several baseball metaphors were used in the meeting, so when the discussion pivoted to cyber insurance, I asked how far along they felt that market was in its development. One CEO said it was only the top of the first inning, and the leadoff batter has just grabbed a bat from the rack before the first pitch has even been thrown – the rest of the room nodded in agreement. We are on the first leg of a long race when it comes to cybersecurity insurance.

There is no question that the expansion of cyber risks and the maturation of the cybersecurity insurance are a tremendous opportunity for the insurance sector to lead in the development of risk-reducing best practices and cyber-hygiene across our national infrastructure. Insurance has a long history of driving best practices and standardization by creating economic incentives through the pricing of products, and the underwriting process can test the risk management techniques and efficacy of a policyholder making a broader range of businesses secure. As insurers develop more sophisticated tools for underwriting and pricing, state regulators will continue to monitor and study cybersecurity products, always remembering that our fundamental commitment is to ensuring that policyholders are protected and treated fairly, and that insurance companies are able to pay claims when they come due.

Conclusion

As insurance markets evolve, state insurance regulators remain extensively engaged with all relevant stakeholders to promote an optimal regulatory framework—cybersecurity insurance is no exception. As the cybersecurity insurance market develops, we remain committed to effective regulation and to making changes when necessary. State insurance regulators will embrace new challenges posed by a dynamic cybersecurity insurance market and we continue to believe that

well-regulated markets make for well-protected policyholders. Thank you again for the opportunity to be here on behalf of the NAIC, and I look forward to your questions.

CYBERSECURITY (EX) TASK FORCE

Adam Hamm, Chair	North Dakota
Raymond G. Farmer	South Carolina
Jim L. Ridling	Alabama
Lori K. Wing-Heier	Alaska
Allen W. Kerr	Arkansas
Dave Jones	California
Marguerite Salazar	Colorado
Katharine L. Wade	Connecticut
Karen Weldin Stewart	Delaware
Stephen C. Taylor	District of Columbia
Kevin M. McCarty	Florida
Gordon I. Ito	Hawaii
Dean Cameron	Idaho
Anne Melissa Dowling	Illinois
Ken Selzer	Kansas
Brian Maynard	Kentucky
Eric A. Cioppa	Maine
Al Redmer, Jr.	Maryland
Mike Rothman	Minnesota
John M. Huff	Missouri
Monica J. Lindeen	Montana
Bruce R. Ramge	Nebraska
Barbara Richardson	Nevada
Roger A. Sevigny	New Hampshire
Peter L. Hartt	New Jersey
John G. Franchini	New Mexico
Maria T. Vullo	New York
Wayne Goodwin	North Carolina
Mary Taylor	Ohio
John D. Doak	Oklahoma
Teresa D. Miller	Pennsylvania
Ángela Weyne	Puerto Rico
Elizabeth Kelleher Dwyer	Rhode Island
Larry Deiter	South Dakota
Julie Mix McPeak	Tennessee
David Mattax	Texas
Todd E. Kiser	Utah
Susan L. Donegan	Vermont
Jacqueline K. Cunningham	Virginia
Mike Kreidler	Washington
Ted Nickel	Wisconsin

NAIC Support Staff: Eric Nordman/Sara Robben/Tony Cotto/Cody Steinwand

Attachment B

Affix Bar Code Above

New Page

CYBERSECURITY AND IDENTITY THEFT INSURANCE COVERAGE SUPPLEMENT

For The Year Ended December 31, 20__
(To Be Filed by April 1)

NAIC Group Code ..... NAIC Company Code .....

Company Name .....

If the reporting entity writes any stand-alone cybersecurity insurance coverage, please provide the following:

1. Stand-Alone Cybersecurity Insurance Policies

Number of Claims Reported		Direct Premiums		Direct Losses		Adjusting and Other Expenses		Direct Defense and Cost Containment		Number of Policies in Force	
1 First Party	2 Third Party	3 Written	4 Earned	5 Paid	6 Incurred	7 Paid	8 Incurred	9 Paid	10 Incurred	11 Claims-Made	12 Occurrence
		$	$	$	$	$	$	$	$		

If the reporting entity writes any stand-alone identity theft insurance coverage, please provide the following:

2. Stand-Alone Identity Theft Insurance Policies

1 Number of Claims Reported	Direct Premiums		Direct Losses		Adjusting and Other Expenses		Direct Defense and Cost Containment		10 Number of Policies in Force
	2 Written	3 Earned	4 Paid	5 Incurred	6 Paid	7 Incurred	8 Paid	9 Incurred	
	$	$	$	$	$	$	$	$	

If the reporting entity writes any cybersecurity insurance coverage that is part of a package policy, please provide the following:

3. Cybersecurity insurance that is part of a package policy

Number of Claims Reported		Direct Losses		Adjusting and Other Expenses		Direct Defense and Cost Containment		Number of Policies in Force	
1 First Party	2 Third Party	3 Paid	4 Case Reserves	5 Paid	6 Case Reserves	7 Paid	8 Case Reserves	9 Claims-Made	10 Occurrence
		$	$	$	$	$	$		

3.1 Can the direct premium earned for the cybersecurity coverage provided as part of a package policy be quantified or estimated? Yes [ ] No [ ]

3.11 If the response to 3.1 is no, please fully explain why the insurer cannot quantify or estimate direct premiums earned:

.....

.....

New Page

CYBERSECURITY AND IDENTITY THEFT INSURANCE COVERAGE SUPPLEMENT (Continued)

For The Year Ended December 31, 20__
(To Be Filed by April 1)

3.2 If the response to question 3.1 is yes, provide the quantified or estimated direct premiums written and direct premium earned amount for cybersecurity insurance included in package policies:

	Cybersecurity Insurance Direct Premiums Written	Cybersecurity Insurance Direct Premiums Earned
3.21 Amount quantified:	$_____	$_____
3.22 Amount estimated using reasonable assumptions:	$_____	$_____

3.3 If the liability portion of a cybersecurity policy is a claims-made policy, is an extended reporting endorsement (tail coverage) offered? Yes [ ] No [ ]

If the reporting entity writes any identity theft insurance coverage that is part of a package policy, please provide the following:

4. Identity theft insurance that is part of a package policy

1 Number of Claims Reported	Direct Losses		Adjusting and Other Expenses		Direct Defense and Cost Containment		8 Number of Policies in Force
	2 Paid	3 Case Reserves	4 Paid	5 Case Reserves	6 Paid	7 Case Reserves	
	$	$	$	$	$	$	

4.1 Can the direct premium earned for the identity theft coverage provided as part of a package policy be quantified or estimated? Yes [ ] No [ ]

4.11 If the response to 4.1 is no, please fully explain why the insurer cannot quantify or estimate direct premiums earned:

.....

.....

4.2 If the response to question 4.1 is yes, provide the quantified or estimated direct premiums written and direct premium earned amount for identity theft insurance included in package policies:

	Identity Theft Insurance Direct Premiums Written	Identity Theft Insurance Direct Premiums Earned
4.21 Amount quantified:	$_____	$_____
4.22 Amount estimated using reasonable assumptions:	$_____	$_____

Principles for Effective Cybersecurity: Insurance Regulatory Guidance[1]

Due to ever-increasing cybersecurity issues, it has become clear that it is vital for state insurance regulators to provide effective cybersecurity guidance regarding the protection of the insurance sector's data security and infrastructure. The insurance industry looks to state insurance regulators to aid in the identification of uniform standards, to promote accountability across the entire insurance sector, and to provide access to essential information. State insurance regulators look to the insurance industry to join forces in identifying risks and offering practical solutions. The guiding principles stated below are intended to establish insurance regulatory guidance that promotes these relationships and protects consumers.

Principle 1: State insurance regulators have a responsibility to ensure that personally identifiable consumer information held by insurers, producers and other regulated entities is protected from cybersecurity risks. Additionally, state insurance regulators should mandate that these entities have systems in place to alert consumers in a timely manner in the event of a cybersecurity breach. State insurance regulators should collaborate with insurers, insurance producers and the federal government to achieve a consistent, coordinated approach.

Principle 2: Confidential and/or personally identifiable consumer information data that is collected, stored and transferred inside or outside of an insurer's, insurance producer's or other regulated entity's network should be appropriately safeguarded.

Principle 3: State insurance regulators have a responsibility to protect information that is collected, stored and transferred inside or outside of an insurance department or at the NAIC. This information includes insurers' or insurance producers' confidential information, as well as personally identifiable consumer information. In the event of a breach, those affected should be alerted in a timely manner.

Principle 4: Cybersecurity regulatory guidance for insurers and insurance producers must be flexible, scalable, practical and consistent with nationally recognized efforts such as those embodied in the National Institute of Standards and Technology (NIST) framework.

Principle 5: Regulatory guidance must be risk-based and must consider the resources of the insurer or insurance producer, with the caveat that a minimum set of cybersecurity standards must be in place for all insurers and insurance producers that are physically connected to the Internet and/or other public data networks, regardless of size and scope of operations.

Principle 6: State insurance regulators should provide appropriate regulatory oversight, which includes, but is not limited to, conducting risk-based financial examinations and/or market conduct examinations regarding cybersecurity.

Principle 7: Planning for incident response by insurers, insurance producers, other regulated entities and state insurance regulators is an essential component to an effective cybersecurity program.

Principle 8: Insurers, insurance producers, other regulated entities and state insurance regulators should take appropriate steps to ensure that third parties and service providers have controls in place to protect personally identifiable information.

[1] These principles have been derived from the Securities Industry and Financial Markets Association's (SIFMA) "Principles for Effective Cybersecurity Regulatory Guidance."

Principle 9: Cybersecurity risks should be incorporated and addressed as part of an insurer's or an insurance producer's enterprise risk management (ERM) process. Cybersecurity transcends the information technology department and must include all facets of an organization.

Principle 10: Information technology internal audit findings that present a material risk to an insurer should be reviewed with the insurer's board of directors or appropriate committee thereof.

Principle 11: It is essential for insurers and insurance producers to use an information-sharing and analysis organization (ISAO) to share information and stay informed regarding emerging threats or vulnerabilities, as well as physical threat intelligence analysis and sharing.

Principle 12: Periodic and timely training, paired with an assessment, for employees of insurers and insurance producers, as well as other regulated entities and other third parties, regarding cybersecurity issues is essential.

W:\National Meetings\2015\Summer\TF\Cybersecurity\Guiding Principle Documents\Final Guiding Principles 4 16 15.docx

National Association of Insurance Commissioners & The Center for Insurance Policy and Research

NAIC Roadmap for Cybersecurity Consumer Protections

This document describes the protections the NAIC believes consumers are entitled to from insurance companies, agents and other businesses when they collect, maintain and use your personal information, including what should happen in connection with a notice that your personal information has been involved in a data breach. Not all of these consumer protections are currently provided for under state law. This document functions as a Consumer Bill of Rights and will be incorporated into NAIC model laws and regulations. If you have questions about data security, a notice you receive about a data breach or other issues concerning your personal information in an insurance transaction, you should contact your state insurance department to determine your existing rights.

As an insurance consumer, you have the right to:

1. Know the types of personal information collected and stored by your insurance company, agent or any business it contracts with (such as marketers and data warehouses).
2. Expect insurance companies/agencies to have a privacy policy posted on their websites and available in hard copy, if you ask. The privacy policy should explain what personal information they collect, what choices consumers have about their data, how consumers can see and change/correct their data if needed, how the data is stored/protected, and what consumers can do if the company/agency does not follow its privacy policy.
3. Expect your insurance company, agent or any business it contracts with to take reasonable steps to keep unauthorized persons from seeing, stealing or using your personal information.
4. Get a notice from your insurance company, agent or any business it contracts with if an unauthorized person has (or it seems likely he or she has) seen, stolen or used your personal information. This is called a *data breach*. This notice should:
   - Be sent in writing by first-class mail or by e-mail if you have agreed to that.
   - Be sent soon after a data breach and never more than 60 days after a data breach is discovered.
   - Describe the type of information involved in a data breach and the steps you can take to protect yourself from identity theft or fraud.
   - Describe the action(s) the insurance company, agent or business it contracts with has taken to keep your personal information safe.
   - Include contact information for the three nationwide credit bureaus.
   - Include contact information for the company or agent involved in a data breach.
5. Get at least one year of identity theft protection paid for by the company or agent involved in a data breach.
6. If someone steals your identity, you have a right to:
   - Put a 90-day initial fraud alert on your credit reports. (The first credit bureau you contact will alert the other two.)
   - Put a seven-year extended fraud alert on your credit reports.
   - Put a credit freeze on your credit report.
   - Get a free copy of your credit report from each credit bureau.
   - Get fraudulent information related to the data breach removed (or "blocked") from your credit reports.
   - Dispute fraudulent or wrong information on your credit reports.
   - Stop creditors and debt collectors from reporting fraudulent accounts related to the data breach.
   - Get copies of documents related to the identity theft.
   - Stop a debt collector from contacting you.

To learn more about the protections in your state or territory, contact your consumer protection office at *https://www.usa.gov/state-consumer* or your state or territory's insurance department at *www.naic.org/state_web_map.htm*.

Standard Definitions Under This Bill of Rights

Data Breach: When an unauthorized individual or organization sees, steals or uses sensitive, protected or confidential information—usually personal, financial and/or health information.

Credit Bureau (Consumer Reporting Agency): A business that prepares credit reports for a fee and provides those reports to consumers and businesses; its information sources are primarily other businesses.

Credit Freeze (Security Freeze): A way you can restrict access to your credit report and prevent anyone other than you from using your credit information.

Personal Information (Personally Identifiable Information): Any information about a consumer that an insurance company, its agents or any business it contracts with maintains that can be used to identify a consumer. Examples include:

- Full name.
- Social Security number.
- Date and place of birth.
- Mother's maiden name.
- Biometric records.
- Driver's license number.

Helpful Links:

"Credit Freeze FAQs" (Federal Trade Commission—FTC) – *www.consumer.ftc.gov/articles/0497-credit-freeze-faqs*

"Disputing Errors on Credit Reports" (FTC) – *www.consumer.ftc.gov/articles/0151-disputing-errors-credit-reports*

"Taking Charge: What to Do If Your Identity Is Stolen" (FTC, May 2012). Tri-fold brochure; online PDF; can order bulk copies at no cost – *https://bulkorder.ftc.gov/system/files/publications/pdf-0009-taking-charge.pdf*

"Know Your Rights" (FTC) – *https://www.identitytheft.gov/know-your-rights.html*

"What Is Identity Theft?" (video; FTC) – *www.consumer.ftc.gov/media/video-0023-what-identity-theft*

"When Information Is Lost or Exposed" (FTC) – *https://www.identitytheft.gov/info-lost-or-stolen.html*

State Consumer Protection Offices (USA.gov) – *www.usa.gov/directory/stateconsumer/index.shtml*

Directory of State Insurance Regulators (NAIC) *www.naic.org/state_web_map.htm*

World's Biggest Data Breaches (information is beautiful) – *www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/*

Draft: 3/2/2016
Draft of New Cybersecurity Model Law
Cybersecurity (EX) Task Force

INSURANCE DATA SECURITY MODEL LAW

Table of Contents

Section 1. Purpose and Intent

The purpose and intent of this Act is to establish the exclusive standards for data security and investigation and notification of a breach of data security applicable to licensees in this state.

Section 2. Applicability and Scope

Consistent with authority to regulate the business of insurance pursuant to the McCarran-Ferguson Act, 15 U.S.C. § 1011 et seq. and the laws of this state, this Act is intended to regulate the business of insurance. No other provision of state or federal law or regulation regarding data security or investigation or notification of a breach of data security shall apply to licensees subject to the provisions of this Act.

Section 3. Definitions

As used in this Act, the following terms shall have these meanings:

A. "Breach of data security," "breach," "data breach," or "security breach" means the unauthorized acquisition of personal information.

The term "breach of data security" does not include the unauthorized acquisition of personal information that is encrypted, redacted, or otherwise protected by another method that renders the information unreadable and unusable if the encryption, redaction, or protection process or key is not also acquired without authorization.

B. "Consumer" means an individual or entity, including but not limited to policyholders and their family members.

C. "Consumer reporting agency" has the same meaning as "consumer reporting agency that compiles and maintains files on consumers on a nationwide basis" in section 603(p) of the Fair Credit Reporting Act (15 U.S.C. 1681a(p)).

D. "Encrypted" means rendered unusable, unreadable, or indecipherable to an unauthorized person through a security technology or methodology generally accepted in the field of information security.

E. "Information security program" means the administrative, technical, or physical safeguards that a licensee uses to access, collect, distribute, process, protect, store, use, transmit, dispose of, or otherwise handle personal information.

F. "Licensee" means all licensed insurers, producers and other persons licensed or required to be licensed, or authorized or required to be authorized, or registered or required to be registered pursuant to the Insurance Law of this state.

G. "Personal Information" means

(1) A financial account number relating to a consumer, including a credit card number or debit card number, in combination with any security code, access code, password, or other personal identification information required to access the financial account; or

(2) Information including:

The first name or first initial and last name of a consumer in combination with:

(a) The consumer's non-truncated social security number;

(b) The consumer's driver's license number, passport number, military identification number, or other similar number issued on a government document used to verify identity;

(c) A user name or e-mail address, in combination with a password or security question and answer that would permit access to an online or financial account of the consumer;

(d) Biometric data of the consumer used to gain access to financial accounts of the consumer;

(e) Health information of the consumer;

(f) Information that the consumer provides to a licensee to obtain an insurance product or service used primarily for personal, family, or household purposes from the licensee;

(g) Information about the consumer resulting from a transaction involving an insurance product or service used primarily for personal, family, or household purposes between a licensee and the consumer;

(h) Information the licensee obtains about the consumer in connection with providing an insurance product or service used primarily for personal, family, or household purposes to the consumer; or

(i) A list, description, or other grouping of consumers (and publicly available information pertaining to them), that is derived using the information described in [Subparagraphs (f) through (h), information provided to licensees] that is not publicly available.

(3) Any information or data except age or gender, that relates to:

(a) The past, present or future physical, mental or behavioral health or condition of a consumer;

(b) The provision of health care to a consumer; or

(c) Payment for the provision of health care to a consumer.

The term "personal information" does not include publicly available information that is lawfully made available to the general public and obtained from federal, state, or local government records; or widely distributed media.

H. "Substantial harm or inconvenience" means

(1) Identity theft; or

(2) Fraudulent transactions on financial accounts.

I. "Third-party service provider" or "service provider" means a person or entity that maintains, processes or otherwise is permitted access to personal information through its provision of services directly to the licensee.

Section 4. Information Security Program

A. Implementation of an Information Security Program

Each licensee shall develop, implement, and maintain a comprehensive written information security program that contains administrative, technical, and physical safeguards for the protection of personal information.

B. Objectives of Information Security Program

A licensee's information security program shall be designed to:

(1) Ensure the security and confidentiality of personal information;

(2) Protect against any anticipated threats or hazards to the security or integrity of the information; and

(3) Protect against unauthorized access to or use of the information that could result in substantial harm or inconvenience to any customer.

C. Appropriateness of Information Security Program

The scale and scope of a licensee's information security program shall be appropriate to:

(1) The size and complexity of the licensee;

(2) The nature and scope of the activities of the licensee; and

(3) The sensitivity of the consumer information to be protected.

D. Risk Assessment

The licensee shall:

(1) Designate an employee or employees to coordinate the information security program;

(2) Identify reasonably foreseeable internal or external threats that could result in unauthorized disclosure, misuse, alteration or destruction of personal information or personal information systems;

(3) Assess the likelihood and potential damage of these threats, taking into consideration the sensitivity of the personal information;

(4) Assess the sufficiency of policies, procedures, personal information systems and other safeguards in place to control these risks, including consideration of risks in each relevant area of the licensee's operations, including:

(a) Employee training and management;

(b) Information systems, including network and software design, as well as information processing, storage, transmission, and disposal; and

(c) Detecting, preventing, and responding to attacks, intrusions, or other systems failures; and

(5) Design and implement information safeguards to control the risks identified in its risk assessment, and regularly assess the effectiveness of the safeguards' key controls, systems, and procedures.

E. Risk Management

The licensee shall:

(1) Design its information security program to control the identified risks, commensurate with the sensitivity of the information, as well as the complexity and scope of the licensee's activities, using as a guide, the *Framework for Improving Critical Infrastructure Cybersecurity* developed by the National Institute of Standards and Technology (NIST), including adopting the following security measures:

(a) Place access controls on information systems, including controls to authenticate and permit access only to authorized individuals and controls to prevent employees from providing personal information to unauthorized individuals who may seek to obtain this information through fraudulent means;

(b) Restrict access at physical locations containing personal information, such as buildings, computer facilities, and records storage facilities, to permit access only to authorized individuals;

(c) Encrypt electronic personal information, including while in transit or in storage on networks or systems to which unauthorized individuals may have access;

(d) Design procedures to ensure that information system modifications are consistent with the licensee's information security program;

(e) Utilize multi-factor authentication procedures, segregation of duties, and employee background checks for employees with responsibilities for, or access to, personal information;

(f) Regularly test or monitor systems and procedures to detect actual and attempted attacks on, or intrusions into, information systems;

(g) Implement response programs that specify actions to be taken when the licensee suspects or detects that unauthorized individuals have gained access to information systems;

(h) Implement measures to protect against destruction, loss, or damage of personal information due to potential environmental hazards, such as fire and water damage or technological failures; and

(i) Develop, implement, and maintain appropriate measures to properly dispose of personal information;

(2) Address cybersecurity risks into the licensee's enterprise risk management process; and

(3) Use an Information Sharing and Analysis Organization (ISAO) to share information and stay informed regarding emerging threats or vulnerabilities.

F. Oversight by Board of Directors

(1) If the licensee has a board of directors, the board or an appropriate committee of the board shall:

(a) Approve the licensee's written information security program; and

(b) Oversee the development, implementation, and maintenance of the licensee's information security program, including assigning specific responsibility for its implementation and reviewing reports from management.

(2) If the licensee has a board of directors, the licensee shall report to its board or an appropriate committee of the board at least annually, the following information:

(a) The overall status of the information security program and the licensee's compliance with this Act; and

(b) Material matters related to its program, addressing issues such as risk assessment, risk management and control decisions, service provider arrangements, results of testing, security breaches or violations and management's responses, and recommendations for changes in the information security program.

G. Oversight of Third-Party Service Provider Arrangements

The licensee shall:

(1) Select and retain third-party service providers that are capable of maintaining appropriate safeguards for the personal information at issue;

(2) Require the third-party service providers to do the following, by contract:

(a) Implement and maintain appropriate safeguards for the personal information at issue, including those security measures listed in [Section 4E(1), Risk Management].

(b) Notify licensee within three (3) calendar days of a discovery of a breach of data security in a system maintained by the third-party service provider that has been contracted to maintain, store, or process data containing personal information on behalf of a licensee;

(c) Indemnify licensee in the event of a cybersecurity incident that results in loss;

(d) Allow licensee or its agents to perform cybersecurity audits of the third-party service provider; and

(e) Represent and warrant its compliance with all requirements; and

(3) Oversee or obtain an assessment of the third-party service provider's compliance with contractual obligations, where appropriate in light of the licensee's risk assessment.

H. Program Adjustments

The licensee shall monitor, evaluate and adjust, as appropriate, the information security program in light of any relevant changes in technology, the sensitivity of its personal information, internal or external threats to information, and the licensee's own changing business arrangements, such as mergers and acquisitions, alliances and joint ventures, outsourcing arrangements and changes to personal information systems.

Section 5. Consumer Rights Before a Breach of Data Security

A. The licensee shall provide consumers with information regarding the types of personal information collected and stored by licensee or any third-party service providers it contracts with.

B. The licensee shall post its privacy policy on its websites and make it available to consumers in hard copy, upon request. The privacy policy shall explain what type of personal information licensee collects, what options consumers have about their data, how consumers can review and change or correct their data if needed, how the data is stored and protected, and what consumers can do if the licensee does not follow its privacy policy.

Section 6. Investigation of a Breach of Data Security

A. If a licensee believes that a breach of data security has or may have occurred in relation to personal information that is maintained, communicated, or otherwise handled by, or on behalf of, the licensee, the licensee shall conduct an investigation.

B. During the investigation, the licensee shall:

(1) Assess the nature and scope of the incident;

(2) Identify any personal information that may have been involved in the incident;

(3) Determine if the personal information has been acquired without authorization; and

(4) Take reasonable measures to restore the security and confidentiality of the systems compromised in the breach.

Section 7. Notification of a Breach of Data Security

A. If the licensee determines under [Section 6, Investigation of a Breach of Data Security] that the unauthorized acquisition of personal information involved in a breach of data security is reasonably likely to cause substantial harm or inconvenience to the consumers to whom the information relates, the licensee, or a third party acting on behalf of the licensee, shall notify, without unreasonable delay:

(1) An appropriate Federal and state law enforcement agency;

(2) The insurance commissioner;

(3) Any relevant payment card network, if the breach involves a breach of payment card numbers;

(4) Each consumer reporting agency that compiles and maintains files on consumers on a nationwide basis, if the breach involves personal information relating to 1,000 or more consumers; and

(5) All consumers to whom the personal information relates.

B. Providing Notice to the Commissioner

No later than five (5) calendar days of identifying a data breach, the licensee shall notify the commissioner, providing as much of the following information as is known to the licensee:

(1) Date of the breach;

(2) Description of the breach, including how the information was lost, stolen, or breached;

(3) How the breach was discovered;

(4) Whether any lost, stolen, or breached information has been recovered and if so, how this was done;

(5) Whether any individuals involved in the incident (both internal and external) have been identified;

(6) Whether a police report has been filed;

(7) Description of the type of information lost, stolen, or breached (equipment, paper, electronic, claims, applications, underwriting forms, medical records etc.);

(8) Whether the information was encrypted;

(9) The time period covered by the information that was lost, stolen or breached;

(10) Number of residents of the state affected by the breach;

(11) Results of any internal review identifying either a lapse in internal procedures or confirmation that all procedures were followed;

(12) Identification of remedial efforts being undertaken to cure the situation which permitted the information security incident to occur;

(13) Copies of the licensee's privacy policies and data breach policy;

(14) Name of a contact person who is both familiar with the details and able to authorize actions for the licensee; and

(15) Other regulatory or law enforcement agencies that have been notified and when notification was provided.

C. Providing Notice to Consumer Reporting Agencies

No later than sixty (60) calendar days of identifying a data breach, the licensee shall notify each consumer reporting agency that compiles and maintains files on consumers on a nationwide basis, if the breach involves personal information relating to [1000] or more consumers.

D. Providing Notice to Consumers

(1) No later than sixty (60) calendar days of identifying a data breach, the licensee shall notify all affected consumers.

(2) Licensee will provide the notification in writing by first-class mail, unless the consumer has agreed to be contacted through e-mail.

(3) No later than forty-five (45) calendar days of identifying a data breach, the licensee shall provide to the commissioner, a draft of the proposed written communication to consumers. The commissioner shall have the right to edit the proposed communication before the licensee sends it to consumers. This proposed notification shall be written in plain English and include the following information:

(a) A description of the type of information involved in the data breach;

(b) A description of the action that the licensee or business it contracts with has taken to safeguard the information;

(c) A summary of rights of victims of identity theft prepared under § 609(d) of the Fair Credit Reporting Act (15 U.S.C. 1681g(d));

(d) The steps consumers can take to protect themselves from identity theft or fraud, which shall include an explanation that consumers shall have a right to do the following:

(i) Put a 90-day initial fraud alert on their credit reports;

(ii) Put a seven-year extended fraud alert on their credit reports;

(iii) Put a credit freeze on their credit report;

(iv) Get a free copy of their credit report from each credit bureau;

(v) Get fraudulent information related to the data breach removed (or "blocked") from their credit reports;

(vi) Dispute fraudulent or wrong information on their credit reports;

(vii) Stop creditors and debt collectors from reporting fraudulent accounts related to the data breach;

(viii) Get copies of documents related to the identity theft; and

(ix) Stop a debt collector from contacting them;

(e) Contact information for the three nationwide consumer reporting agencies;

(f) Contact information for the licensee or its designated call center; and

(g) An offer from the licensee to the consumer to provide appropriate identity theft protection services free of cost to the consumer for a period of not less than twelve (12) months.

E. Providing Notice Regarding Breaches of Third-Party Service Providers

Licensee shall comply with [Subsections B and D] by notifying the commissioner and consumers in the event of a breach of data security in a system maintained by a third-party service provider. The computation of licensee's deadlines shall begin on the day the third-party service provider provides notice to licensee.

F. Notwithstanding the requirements of [Subsections C, D, and E], notice may be delayed where requested by an appropriate state or federal law enforcement agency. The commissioner shall be notified of any such request.

Section 8. Consumer Protections Following a Breach of Data Security

After reviewing the licensee's data breach notification, the commissioner shall prescribe the appropriate level of consumer protection required following the data breach and for what period of time that protection will be provided. At a minimum, the licensee will offer to pay for at least twelve (12) months of identity theft protection for affected consumers.

Section 9. Power of Commissioner

The commissioner shall have power to examine and investigate into the affairs of any licensee to determine whether the licensee has been or is engaged in any conduct in violation of this Act. This power is in addition to the powers which the commissioner has under [insert applicable statutes governing the examination of insurers]. Any such examination shall be conducted pursuant to [insert applicable statutes governing the examination of insurers].

Section 10. Hearings, Witnesses, Appearances, Production of Books and Service of Process

A. Whenever the commissioner has reason to believe that a licensee has been or is engaged in conduct in this state which violates this Act, the commissioner shall issue and serve upon such licensee a statement of charges and notice of hearing to be held at a time and place fixed in the notice. The date for such hearing shall be not less than [insert number] days after the date of service.

B. At the time and place fixed for such hearing the licensee charged shall have an opportunity to answer the charges against it and present evidence on its behalf. Upon good cause shown, the commissioner shall permit any adversely affected person to intervene, appear and be heard at such hearing by counsel or in person.

C. At any hearing conducted pursuant to this section, the commissioner may administer oaths, examine and cross-examine witnesses and receive oral and documentary evidence. The commissioner shall have the power to subpoena witnesses, compel their attendance and require the production of books, papers, records, correspondence and other documents which are relevant to the hearing. A stenographic record of the hearing shall be made upon the request of any party or at the discretion of the commissioner. If no stenographic record is made and if judicial review is sought, the commissioner shall prepare a statement of the evidence for use on the review. Hearings conducted under this section shall be governed by the same rules of evidence and procedure applicable to administrative proceedings conducted under the laws of this state.

D. Statements of charges, notices, orders and other processes of the commissioner under this Act may be served by anyone duly authorized to act on behalf of the commissioner. Service of process may be completed in the manner provided by law for service of process in civil actions or by registered mail. A copy of the statement of charges, notice, order or other process shall be provided to the person or persons whose rights under this Act have been allegedly violated. A verified return setting forth the manner of service, or return postcard receipt in the case of registered mail, shall be sufficient proof of service.

Section 11. Confidentiality

A. Any documents, materials or other information in the control or possession of the department of insurance that is furnished by a licensee or an employee or agent thereof acting on behalf of licensee, or obtained by the insurance commissioner in an investigation pursuant to this Act shall be confidential by law and privileged, shall not be subject to [insert open records, freedom of information, sunshine or other appropriate phrase], shall not be subject to subpoena, and shall not be subject to discovery or admissible in evidence in any private civil action. However, the insurance commissioner is authorized to use the documents, materials or other information in the furtherance of any regulatory or legal action brought as a part of the insurance commissioner's duties.

B. Neither the insurance commissioner nor any person who received documents, materials or other information while acting under the authority of the insurance commissioner shall be permitted or required to testify in any private civil action concerning any confidential documents, materials, or information subject to [Subsection A].

C. In order to assist in the performance of the insurance commissioner's duties under this Act, the insurance commissioner:

(1) May share documents, materials or other information, including the confidential and privileged documents, materials or information subject to [Subsection A], with other state, federal, and international regulatory agencies, with the National Association of Insurance Commissioners, its affiliates or subsidiaries, and with state, federal, and international law enforcement authorities, provided that the recipient agrees to maintain the confidentiality and privileged status of the document, material or other information;

(2) May receive documents, materials or information, including otherwise confidential and privileged documents, materials or information, from the National Association of Insurance Commissioners, its affiliates or subsidiaries and from regulatory and law enforcement officials of other foreign or domestic jurisdictions, and shall maintain as confidential or privileged any document, material or information received with notice or the understanding that it is confidential or privileged under the laws of the jurisdiction that is the source of the document, material or information; and

(3) **[OPTIONAL]** May enter into agreements governing sharing and use of information consistent with this subsection.

D. No waiver of any applicable privilege or claim of confidentiality in the documents, materials, or information shall occur as a result of disclosure to the commissioner under this section or as a result of sharing as authorized in [Subsection C].

E. Nothing in this Act shall prohibit the insurance commissioner from releasing final, adjudicated actions including for cause terminations that are open to public inspection pursuant to [insert appropriate reference to state law] to a database or other clearinghouse service maintained by the National Association of Insurance Commissioners, its affiliates or subsidiaries of the National Association of Insurance Commissioners.

Section 12. Cease and Desist Orders and Reports

A. If, after a hearing pursuant to Section [section on hearings], the commissioner determines that the licensee charged has engaged in conduct or practices in violation of this Act, the commissioner shall reduce his or her findings to writing and shall issue and cause to be served upon such licensee a copy of such findings and an order requiring such licensee to cease and desist from the conduct or practices constituting a violation of this Act.

B. If, after a hearing pursuant to Section [section on hearings], the commissioner determines that the licensee charged has not engaged in conduct or practices in violation of this Act, the commissioner shall prepare a written report which sets forth findings of fact and conclusions of law. Such report shall be served upon the licensee charged and upon the person or persons, if any, whose rights under this Act were allegedly violated.

C. Until the expiration of the time allowed under Section [section on judicial review] of this Act for filing a petition for review or until such petition is actually filed, whichever occurs first, the commissioner may modify or set aside any order or report issued under this section. After the expiration of the time allowed under Section [section on judicial review] of this Act for filing a petition for review, if no such petition has been duly filed, the commissioner may, after notice and opportunity for hearing, alter, modify or set aside, in whole or in part, any order or report issued under this section whenever conditions of fact or law warrant such action or if the public interest so requires.

Section 13. Penalties

A. In any case where a hearing pursuant to Section [section on hearings] results in the finding of a knowing violation of this Act, the commissioner may, in addition to the issuance of a cease and desist order as prescribed in Section [section on cease and desist orders], order payment of a monetary penalty of not more than [$500] for each violation but not to exceed [$10,000] in the aggregate for multiple violations.

B. Any person who violates a cease and desist order of the commissioner under Section [section on cease and desist orders] of this Act may, after notice and hearing and upon order of the commissioner, be subject to one or more of the following penalties, at the discretion of the commissioner:

(1) A monetary fine of not more than [$10,000] for each violation;

(2) A monetary fine of not more than [$50,000] if the commissioner finds that violations have occurred with such frequency as to constitute a general business practice; or

(3) Suspension or revocation of an insurance institution's or agent's license.

C. Notwithstanding the foregoing, nothing in this Act shall be construed to limit the commissioner's authority under [insert citation to Unfair Trade Practices Act].

Section 14. Judicial Review of Orders and Reports

A. Any licensee subject to an order of the commissioner under Section [section on cease and desist orders] or Section [section on penalties] or any licensee whose rights under this Act were allegedly violated may obtain a review of any order or report of the commissioner by filing in the [insert title] Court of [insert county] County, within [insert number] days from the date of the service of such order or report, a written petition requesting that the order or report of the commissioner be set aside. A copy of such petition shall be simultaneously served upon the commissioner, who shall forthwith certify and file in such court a transcript of the entire record of the proceeding giving rise to the order or report which is the subject of the petition. Upon filing of the petition and transcript the [insert title] Court shall have jurisdiction to make and enter a decree modifying, affirming or reversing any order or report of the commissioner, in whole or in part. The findings of the commissioner as to the facts supporting any order or report, if supported by clear and convincing evidence, shall be conclusive.

B. To the extent an order or report of the commissioner is affirmed, the court shall issue its own order commanding obedience to the terms of the order or report of the commissioner. If any party affected by an order or report of the commissioner shall apply to the court for leave to produce additional evidence and shall show to the satisfaction of the court that such additional evidence is material and that there are reasonable grounds for the failure to produce such evidence in prior proceedings, the court may order such additional evidence to be taken before the commissioner in such manner and upon such terms and conditions as the court may deem proper. The commissioner may modify his or her findings of fact or make new findings by reason of the additional evidence so taken and shall file such modified or new findings along with any recommendation, if any, for the modification or revocation of a previous order or report. If supported by clear and convincing evidence, the modified or new findings shall be conclusive as to the matters contained therein.

C. An order or report issued by the commissioner under Section [section on cease and desist orders] or [section on penalties] shall become final:

(1) Upon the expiration of the time allowed for the filing of a petition for review, if no such petition has been duly filed; except that the commissioner may modify or set aside an order or report to the extent provided in Section [section on cease and desist orders]; or

(2) Upon a final decision of the [insert title] Court if the court directs that the order or report of the commissioner be affirmed or the petition for review dismissed.

D. No order or report of the commissioner under this Act or order of a court to enforce the same shall in any way relieve or absolve any licensee affected by such order or report from any liability under any law of this state.

Section 15. Individual Remedies

A. If any licensee fails to comply with Section [insert section(s) addressing consumer rights] of this Act with respect to the rights granted under those sections, any person whose rights are violated may apply to the [insert title] Court of this state, or any other court of competent jurisdiction, for appropriate equitable relief.

B. In any action brought pursuant to this section, the court may award the cost of the action and reasonable attorney's fees to the prevailing party.

C. An action under this section must be brought within two (2) years from the date the alleged violation is or should have been discovered.

D. Except as specifically provided in this Act, there shall be no remedy or recovery available to consumers, in law or in equity, for occurrences constituting a violation of any provisions of this Act.

Section 16. Immunity

No cause of action in the nature of defamation, invasion of privacy or negligence shall arise against any person for disclosing personal or privileged information in accordance with this Act, nor shall such a cause of action arise against any person for furnishing personal or privileged information to a licensee; provided, however, this section shall provide no immunity for disclosing or furnishing false information with malice or willful intent to injure any person.

Section 17. Obtaining Information Under False Pretenses

Any person who knowingly and willfully obtains information about a consumer from a licensee under false pretenses shall be fined not more than [$10,000] or imprisoned for not more than one year, or both.

Section 18. Rules and Regulations

The commissioner may, upon notice and opportunity for all interested persons to be heard, issue such rules, regulations and orders as shall be necessary to carry out the provisions of this Act.

Section 19. Severability

If any provisions of this Act or the application thereof to any person or circumstance is for any reason held to be invalid, the remainder of the Act and the application of such provision to other persons or circumstances shall not be affected thereby.

Section 20. Effective Date

This Act shall take effect on [insert a date which allows at least a one year interval between the date of enactment and the effective date].