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

May 14, 2015

Chairman Jeb Hensarling
U.S. House of Representatives
Committee on Financial Services
2129 Rayburn House Office Building
Washington, DC 20515

Ranking Member Maxine Waters
U.S. House of Representatives
Committee on Financial Services
4340 O'Neill Federal Office Building
Washington, DC 20515

Re: Insurance Consumer Data Protection

Dear Chairman Hensarling and Ranking Member Waters:

On behalf of the National Association of Insurance Commissioners (NAIC)[1], we write today to thank you for holding a hearing on "Protecting Consumers: Financial Data Security in the Age of Computer Hackers." State insurance regulators take very seriously our responsibility to ensure the entities we regulate are protecting the many kinds of highly sensitive consumer information they retain. In this regard, we are acutely aware of the complex mission insurance regulators have of protecting consumers, laying out expectations for the insurance industry, and recognizing the economy-wide role insurers can play in driving best practices and mitigating the financial aftermath of a cyber attack.

As you know, insurance companies in the United States are subject to a stringent state-based regulatory regime designed with the primary mission of protecting policyholders. Consumer data privacy and cybersecurity issues are not new to state insurance regulators – the NAIC's *Standards for Safeguarding Consumer Information Model Regulation* sets forth standards that insurance entities must meet to be in compliance with federal and state information security laws and regulations, and the NAIC examiner handbooks for financial and market conduct exams include extensive guidance on examining controls to confirm insurance entities are taking necessary steps to protect consumers. Even when an insurer is diligent to secure infrastructure, they may be the victim of a criminal data breach. In such an event, companies are required to inform insurance regulators in all affected states, at which point we work with law enforcement agencies and the affected company to ensure consumers are notified promptly and steps are taken to mitigate potential harm.

[1] Founded in 1871, the NAIC is the U.S. standard-setting and regulatory support organization created and governed by the chief insurance regulators from the 50 states, the District of Columbia and the five U.S. territories. Through the NAIC, state insurance regulators establish standards and best practices, conduct peer review, and coordinate their 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.

Last November, following numerous discussions about cybersecurity among our members and leadership, the NAIC established a Cybersecurity (EX) Task Force.[2] After announcing its membership[3] this February, the Task Force laid out an ambitious work plan, and while much work remains, we have already made significant progress in our efforts to enhance cybersecurity protections in insurance.
Following extensive written and verbal comments by interested parties, on April 16, 2015 the Task Force approved a finalized list of 12 insurance regulatory guiding principles.[4] We believe these principles create a broad framework to lay out our duties and obligations as regulators and the expectations we have for our sector. The principles will promote accountability across the entire insurance sector in the best interests of consumers. They will serve as the foundation for protection of sensitive consumer information held by insurers and producers while guiding the regulators who oversee the insurance industry.

The Task Force also worked with the NAIC's Property and Casualty (C) Committee to draft a Cybersecurity Insurance Coverage Supplement proposal for the annual financial statement required of insurers.[5] This filing will provide regulators with more specific information regarding the size of the growing cyber liability market on a nationwide basis. The draft proposal was exposed for comment in March, and is currently under review by several NAIC committees. Additionally, the Task Force is working closely with the Information Technology Examination (E) Working Group to update examination protocols for financial examiners to ensure that cyber security is embedded in on-site examinations of insurers. Similar updated protocols for market conduct examiners are also under consideration.

Additional Task Force plans for the immediate future include a survey of states to assess cyber vulnerabilities, development of a "Consumer Bill of Rights" for insurance data breach victims, webinars on the benefits of information sharing, and a comprehensive review of existing cybersecurity related model laws and regulations.

Consumers have a right to expect that personal financial and health information entrusted to insurers and health care providers is secure. As Congress contemplates legislation in this arena, we encourage you not to limit state regulators' tools or authorities to protect policyholders. While we understand and appreciate the potential benefits of establishing common definitions and cross-sector minimum standards for data security, we remain skeptical of any efforts that involve preemption of a state's right to enact protections for its insurance consumers that go above and beyond those recommended or required by Federal law. We also are concerned with efforts to limit individual state regulators from protecting consumers in their state, regardless of where a breached insurer is domiciled. While well intentioned, such standards may actually undermine existing consumer protections, as well as inhibit future enhancements and innovation necessary for regulators and companies to adapt to evolving threats.

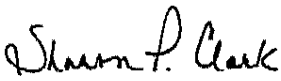
The American public relies on insurance for financial peace of mind, and state insurance regulators are committed to continuing our leadership in this area to maintain the trust of policyholders across the country. We commend your Committee for its attention to the critical issue of consumer data protection, and look forward to working with you to design a strong data protection framework that is in the best interests of insurance consumers.

[2] Attachment A – NAIC Press Release, November 19, 2014.
[3] Attachment B – Cybersecurity (EX) Task Force Membership List
[4] Attachment C – Adopted Principles for Effective Cybersecurity: Insurance Regulatory Guidance
[5] Attachment D – Proposed Cybersecurity Insurance Coverage Supplement

Sincerely,

Monica J. Lindeen
NAIC President
Montana Commissioner of
Securities and Insurance

John M. Huff
NAIC President-Elect
Director of Missouri's Department of Insurance,
Financial Institutions, and Professional Registration



Sharon P. Clark
NAIC Vice President
Kentucky Insurance Commissioner

Theodore K. Nickel
NAIC Secretary-Treasurer
Wisconsin Insurance Commissioner

E. Benjamin Nelson
NAIC Chief Executive Officer

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

NEWS RELEASE

FOR IMMEDIATE RELEASE

INSURANCE REGULATORS ESTABLISH CYBERSECURITY TASK FORCE

NAIC forms committee to address emerging issues related to cyber threats

WASHINGTON, D.C. (Nov. 19, 2014) -Today the National Association of Insurance Commissioners (NAIC) formed a special task force to help coordinate insurance issues related to cybersecurity. The task force will make recommendations and coordinate NAIC efforts regarding: the protection of information housed in insurance departments and the NAIC; the protection of consumer information collected by insurers; and collecting information on cyber-liability policies being issued in the marketplace. The group will report and make recommendations to the Executive Committee.

"The threat of a cyber-attack is very real, and state regulators are committed to developing the tools we need to ensure effective regulation in this area," said Adam Hamm, NAIC President and North Dakota Insurance Commissioner. "The American public relies on insurance for financial peace of mind, and our leadership in this area is critical to maintaining that trust."

The creation of the task force is a reflection of the NAIC's growing commitment to addressing cyber security in the insurance sector. State regulators serve on the Treasury Department's Financial Banking and Information Infrastructure Committee and on the Executive Branch and Independent Agency Regulatory Cybersecurity Forum, where they work with Federal regulators to address cyber threats in the U.S. Earlier this year, the NAIC hosted a forum on regulatory challenges as they relate to cybersecurity.

About the NAIC

The National Association of Insurance Commissioners (NAIC) is the U.S. 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, state insurance regulators establish standards and best practices, conduct peer review, and coordinate their regulatory oversight. NAIC staff supports these efforts and represents the collective views of state regulators domestically and internationally. NAIC members, together with the central resources of the NAIC, form the national system of state-based insurance regulation in the U.S. For more information, visit www.naic.org.

Contacts

Communications Division
news@naic.org

Scott Holeman
Communications Director

Jeremy Wilkinson
Sr. Electronic Communications Manager

Miun Gleeson
Sr. Communications Specialist

Erin Yang
Media Strategist

Katherine Jones
Communications Specialist

Visit the NEWSROOM for media resources, archived releases and alerts

Join Our E-mail List to receive the latest news releases and other information from the NAIC Communications Division.

CYBERSECURITY (EX) TASK FORCE

Adam Hamm, Chair	North Dakota
Raymond G. Farmer, Vice Chair	South Carolina
Jim L. Ridling	Alabama
Lori K. Wing-Heier	Alaska
Germaine L. Marks	Arizona
Dave Jones	California
Katharine L. Wade	Connecticut
Chester McPherson	District of Columbia
Kevin McCarty	Florida
Gordon I. Ito	Hawaii
James Stephens	Illinois
Eric A. Cioppa	Maine
Al Redmer Jr.	Maryland
Mike Rothman	Minnesota
John M. Huff	Missouri
Monica J. Lindeen	Montana
Bruce R. Ramge	Nebraska
Scott J. Kipper	Nevada
Roger A. Sevigny	New Hampshire
Kenneth E. Kobylowski	New Jersey
Benjamin M. Lawsky	New York
Mark O. Rabauliman	Northern Mariana Islands
Mary Taylor	Ohio
John D. Doak	Oklahoma
Teresa D. Miller	Pennsylvania
Joseph Torti III	Rhode Island
David Mattax	Texas
Jaqueline K Cunningham	Virginia
Mike Kreidler	Washington
Ted Nickel	Wisconsin

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

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

CYBERSECURITY 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 cybersecurity coverage, please provide the following:

1. Standalone Policies

Direct Premiums		Direct Losses		Direct Defense and Cost Containment		Number of Policies in Force	
1 Written	2 Earned	3 Paid	4 Incurred	5 Paid	6 Incurred	7 Claims Made	8 Occurrence
$	$	$	$	$	$		

1.1 What is the range of the limits offered for the standalone policy? $_____ to $_____

2. Commercial Multiple Peril Package Policies:

2.1 Does the reporting entity provide cybersecurity coverage as part of a package policy? Yes[ ] No[ ]

2.2 If the answer to 2.1 is yes, please provide the following:

Direct Losses		Direct Defense and Cost Containment		Number of Policies with cybersecurity coverage in Force	
1 Paid	2 Paid + Change in Case Reserves	3 Paid	4 Paid + Change in Case Reserves	5 Claims Made	6 Occurrence
$	$	$	$		

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

2.4 If the answer to question 2.3 is yes, provide the quantified or estimated direct premium earned amount for cybersecurity coverage included in package policies

2.41 Amount quantified: $_____

2.42 Amount estimated using reasonable assumptions: $_____

2.5 What is the range of limits offered for the cybersecurity policies? $_____ to $_____

3. If the cybersecurity policy is a Claims Made policy, is tail coverage offered? Yes[ ] No[ ]

3.1 If tail coverage is offered, what is the range of the limits offered? $_____ to $_____

CYBERSECURITY INSURANCE COVERAGE SUPPLEMENT

This supplement should be completed by those reporting entities that provide cybersecurity coverage in a standalone policy or as part of a commercial multiple peril package policy. The supplement should be reported on a direct basis (before assumed and ceded reinsurance).

Cybersecurity

Coverage for damages arising out of unauthorized use of, or unauthorized access to, electronic data or software within your network or business.

Line 1 Direct premiums, losses and defense and cost containment expenses for standalone policies are to be reported before reinsurance for columns 1 through 6.

For columns 7 and 8, provide the number of in force standalone policies that are claims made vs. occurrence.

Line 1.1 Provide the range of the limits offered for standalone policies.

Line 2.2 Direct losses and defense and cost containment expenses for commercial multiple peril package policies are to be reported before reinsurance for Columns 1 through 4.

For Columns 5 and 6, provide the number of in force multiple peril policies containing cybersecurity coverage that are claims made vs. occurrence.

Line 2.4 If the answer to 2.3 is "yes," provide the amount of direct premium earned (qualified or estimated) for cybersecurity coverage included in package policies before reinsurance.

Line 2.5 Provide the range of limits offered for the commercial multiple peril package cybersecurity policies

Line 3.1 If the answer to 3 is yes, provide the range of limits offered for tail coverage.