Comments of
the Center for Economic Justice
the Consumer Federation of America
United Policyholders and
the National Consumer Law Center (on behalf of its low-income clients)

on March 12, 2015

NAIC Draft Principles for Effective Cybersecurity Insurance Regulatory Guidance

CEJ, CFA, UP and NCLC offer the following comments on the March 12, 2015 draft "Principles for Effective Cybersecurity Regulatory Guidance."

We commend state insurance regulators for addressing issues of cybersecurity of entities regulated by state insurance departments. The issue has grown in importance for both market regulation and financial oversight because insurers and producers are collecting far greater amounts of personal consumer information today than even ten years ago. Today, a data breach of an insurer puts huge amounts of personal, non-insurance consumer information at risk in addition to insurance information. This greater amount of data in the hands of fraudsters puts consumers at greater risk of identity theft as well as scams directed at consumers. In addition, greater amounts of personal consumer data collected by insurers means greater financial risks to insurers from data breaches, including the costs of responding to and addressing data breaches (such as contacting consumers whose personal information has been stolen, dealing with new information to protect consumer privacy and repairing and strengthening data systems). The financial risks go beyond the costs of dealing with a data breach and can include reputational risk and hacker fraud directed at the insurer. The challenge to state insurance regulators is great – in large part because insurance regulatory practices have not kept up with the increased data collection (big data and data mining) practices of insurers. Consequently, vital consumer protections are not in place.

A fundamental omission from the draft principles is that they never explicitly state the requirement for insurers and producers to comply with existing state data security and breach laws. While such a principle may be a given, it would be helpful to remind the insurance industry that complying with existing laws is a bare minimum, but that more may be expected from an industry that holds so much confidential, sensitive information of consumers.

We note that the draft principles were derived from "Principles for Effective Cybersecurity Regulatory Guidance" published by the Securities Industry and Financial Markets Association. SIFMA is an organization of broker-dealers, banks and asset managers. SIFA describes itself as the "voice of the nation's securities industry." Not surprisingly, the SIFMA principles reflect the perspective of businesses who collect and maintain personal consumer information related to the sale of financial products. The SIFMA principles do not reflect the views or needs of consumers whose personal information is collected and put at risk by these organizations. It is unclear why the SIFMA principles were chosen as the basis for cybersecurity policy of state insurance regulators.

We also note that the SIFMA document contains discussion of each principle. This discussion is essential to understand and interpret the terminology used in the principles. The draft NAIC principles copy terms from SIFMA like "guidance must be flexible, scalable and practical" and "guidance is risk-based and threat-informed." While the SIFMA document attempts to explain these concepts, the draft NAIC document does not, with the result that the NAIC principles use vague terms with no explanation such that different stakeholders will read into the principles what the stakeholder wants.

Specific Comments

We copy the text of the draft and use redline to show our suggested edits, followed by comments to explain the edits.

> Due to ever increasing cybersecurity issues, it has become clear that it is vital for insurance regulators to provide effective cybersecurity guidance regarding the protection of the insurance sector's data security and infrastructure. ~~The insurance regulators commend insurance companies for conducting a review of their cybersecurity policies, regulations, and guidance with the goal of strengthening the insurance sector's defense and response to cyber-attacks.~~ The insurance industry looks to the insurance regulators to aid in the identification of uniform standards, promoting accountability across the entire insurance sector, and to provide access to essential information. The insurance regulators also depend upon the insurance industry and the consumers whose personal information is collected and at risk, to join forces to~~in~~ identify~~ing~~ risks and ~~the~~ offer~~ing~~ of practical solutions. The guiding principles stated below are intended to establish insurance regulatory guidance that promotes these relationships and protects consumers and the insurance industry.

Comment: We suggest deletion of the second sentence. First, it is unclear what substantive efforts insurance companies have taken to prevent cyberattacks and protect personal consumer information and if the data protection efforts have matched insurer data collection activities. Second, even if such a commendation was warranted, it is out of place in a document outlining regulatory guidance principles.

We also suggest adding a phrase identifying consumers, whose personal information is collected and at risk, as a stakeholder.

Principle 1: Insurance regulators have a ~~significant role and~~ responsibility ~~regarding~~ to ensure personal consumer information held by insures and producers is protected from ~~protecting consumers from~~ cybersecurity risks and that systems are in place to quickly alert consumers when that personal information has been stolen from insurers and producers.

Comment: If regulators have a responsibility, then clearly regulators have a role. It is redundant to use both terms. The principle as drafted is quite vague. Our suggested edits make clear what the threat is and what the regulators' responsibilities are. Our proposed edits capture the intent of both principles 1 and 2.

Principle 2 ~~Insurance regulators have a significant role and responsibility regarding the insurers' efforts to protect sensitive customer health and financial information.~~ Insurers and producers have a responsibility to policyholders, applicants and claimants to inform these consumers of the specific personal information maintained by the insurer or producer on a periodic basis and in the event the personal information is stolen from the insurer or producer. The disclosure to consumers should itemize the personal information to enable the consumers to better respond to the theft of their personal information

Comment: The original draft principle 2 is captured in our suggested edits to principle 1. We proposed a new principle because insurers and producers have a responsibility to policyholders, applicants and claimants to inform these consumers of the specific personal information maintained by the insurer or producer on a periodic basis and in the event the personal information is stolen from the insurer or producer. The disclosure to consumers should itemize the personal information to enable the consumers to better respond to the theft of their personal information. The addition of this principle is essential to presenting a balanced approach that considers the interests of all stakeholders – those whose personal information is collected and at risk and those responsible for protecting that information.

Principle 3: Insurance regulators have a ~~significant role and~~ responsibility to~~in~~ protect~~ing~~ the confidential~~sensitive~~ information of insurers, produces and consumers maintained in insurance departments and at the NAIC and to quickly alert consumers, insurers and producers when that confidential information has been stolen from the insurance department or the NAIC.

Comment: We suggest replacing "sensitive" with "confidential" since there are statutory requirements regarding protection of confidential information and confidential information is the terminology used in state open records laws. We also suggest state regulators have a responsibility both to protect the confidential information and to alert entities in the event of a data breach.

Principle 4: ~~Insurance regulators recognize the value of collaboration in the development of regulatory guidance with insurers, insurance producers, consumers and the federal government with the goal of a consistent, coordinated national approach.~~

Comment: "Recognizing the value" is not a principle. The recognition of the need for collaboration is reflected in action, such as exposing this document for comment as well as the other substantive principles requiring collaboration.

Principle 5: Compliance with cybersecurity regulatory guidance ~~must be flexible, scalable, practical and~~ consistent with the national efforts embodied in the National Institute of Standards and Technology (NIST) framework.

Comment: It is unclear what it means for compliance with regulatory guidance to be "flexible, scalable and practical." If these terms have substantive meaning, then the document should provide some explanation of the terms. In any event, compliance should ensure reasonable protection of personal consumer information. If such efforts are not "practical" for the insurer or producer, then the insurer or producer should not be collecting and maintaining the information.

Principle 6: ~~Regulatory guidance must consider the resources of the insurer or insurance producer.~~

Comment: This principle is taken from SIFMA and reflects the one-sided perspective of SIFMA. Regulatory guidance should consider the potential harm to consumers. If the insurer or producer does not have the resources to protect consumers' personal financial information, the insurer or producer should not be holding that information.

Principle 7: ~~Effective cybersecurity guidance must be risk-based and threat-informed.~~

Comment: This principle is taken from SIFMA. While the terms "risk-based and threat-informed" are catchy, it is unclear what they mean or how they would shape regulatory guidance. Unless these terms are defined or translated into meaningful language, the principle should be deleted.

Principle 8: Insurance regulators should provide appropriate regulatory oversight~~,~~ by auditing insurer and producer cybersecurity capabilities that go beyond the use of checklists or other self-reporting mechanisms ~~which includes but is not limited to, conducting risk-based, value-added financial examinations and/or market conduct examinations regarding cybersecurity.~~

Comment: The terms "risk-based" and "value-added" are taken from SIFMA. It is unclear what "value-added" means in terms of examinations or who would perform that calculation. The core concept of the SIFMA principle (upon which this language is based) refers to the use of audits instead of check lists. We agree.

Principle 9: Planning for crisis response for insurance regulators, insurers, and insurance producers is an essential component to an effective cybersecurity program.

Principle 10: The effective management of cybersecurity by third parties and service providers used by insurers and producers is essential for protection of consumer's sensitive personal health and financial information.

Principle 11 Information sharing is important for risk management purposes; however, it must be limited to essential cybersecurity information and protect sensitive confidential information. ???

Comment: It is unclear what parties are included in the information sharing in this principle or what is means to limit sharing to "essential cybersecurity information."

Principle 12 Cybersecurity risks should be included and addressed as part of an insurers and insurance producers Enterprise Risk Management processes.

Principle 13 High level information technology internal audit findings should be discussed at the insurers and insurance producers Board of Director meetings.

Principle 14 It is essential for insurers and insurance producers to join Financial Services Information Sharing and Analysis Center (FSISAC) to share information and stay informed about cyber and physical threat intelligence analysis and sharing.

Principle 15 Sensitive data collected, ~~and~~ stored and transferred inside or outside of an insurer's or insurance producer's network should be encrypted.

Principle 16 Periodic and timely training for employees of insurers and insurance producers regarding cybersecurity issues is essential.

Principle 17 Enhanced market regulation~~solvency~~ oversight is needed for insurers selling cyber insurance to businesses and families.

Comment: As opposed to enhanced solvency oversight tools for ***cyberthreats***, it is unclear why enhanced solvency oversight is needed for cyberinsurance, what makes cyberinsurance a unique threat to insurer solvency or why traditional solvency oversight tools are inadequate for cyberinsurance. On the other hand, since some existing commercial policies currently provide some coverage for cyberliabilities, and new products are emerging that are advertised to provide insurance specifically for data breaches, enhanced market regulation/product oversight seems imperative. We have seen the sale of useless "identify theft" products to vulnerable consumers barraged with warnings about the harms of identity theft. Our concern is as great or greater for small and medium-sized businesses purchasing new cyberinsurance coverage. The fact that cyberinsurance is a new product in an area with limited understanding by personal and commercial policyholders calls for enhanced market regulation, including careful review of policy contracts to ensure they provide substantive coverage, are not deceptive and are not duplicative of existing coverage from other commercial policies.

Principle 18 Insurance regulators should collect~~Additional~~ data related to ~~on the sale of~~ cyber insurance product sales, claims and reserving practices to ensure effective prudential and market conduct oversight. ~~should be collected to assist insurance regulators with oversight of financial and market regulation.~~

Comment: We suggest revised wording to make it clear that insurance regulators should be collecting information and that the data should cover more than sales.