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

February 17, 2017

Legislative and Regulatory Activities Division
Office of the Comptroller of the Currency
400 7th Street SW
Suite 3E-218
Washington, D.C. 20219

Robert deV. Frierson
Secretary
Board of Governors of the Federal Reserve System
20th Street and Constitution Avenue NW
Washington, D.C. 20551

Robert E. Feldman
Executive Secretary
Federal Deposit Insurance Corporation
550 17th Street NW
Washington, D.C. 20429

Re: Enhanced Cyber Risk Management Standards; Docket No. R-1550 and RIN 7100-AE 61; Docket ID OCC-2016-0016; RIN 3064-AE45

Dear Sirs:

On behalf of the National Association of Insurance Commissioners (NAIC),[1] we write today regarding the joint advance notice of proposed rulemaking on "Enhanced Cyber Risk Management Standards." State insurance regulators are keenly aware of the potentially devastating effects cyber-attacks can have and share the Agencies' commitment to addressing cybersecurity risks. Given the financial sector's increasing technology dependence and interconnectedness, we believe it is important that the Agencies coordinate with state insurance regulators in an effort to strive for consistency to align our cyber regulatory guidance where possible and appropriate. Coordination is particularly pertinent for the insurance groups in which we share regulatory oversight. As you move forward with drafting specific standards, we encourage close consultation so that we can cooperatively develop cybersecurity frameworks to address the challenges of cyber risk management.

With regard to the insurance sector, state insurance regulators have taken a number of steps to enhance data security expectations to ensure the insurers, agents, and brokers we regulate are adequately protecting the many kinds of highly sensitive consumer financial and health information they retain. As part of these efforts, state insurance regulators, through the NAIC, formed a Cybersecurity Task Force in 2014, to serve as the central focus for insurance regulatory activities related to cybersecurity. Through the Task Force, the NAIC developed twelve Principles for Effective Cybersecurity[2] that set forth the framework through which insurance regulators will evaluate efforts by insurers, producers, and other regulated entities to protect consumer information

[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.

[2] Attachment A - NAIC *Principles for Effective Cybersecurity: Insurance Regulatory Guidance*, April 2015

entrusted to them. The NAIC also adopted a Roadmap for Consumer Cybersecurity Protections[3] to describe protections state insurance regulators believe 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.

Further, we have updated and strengthened existing guidance for examiners regarding IT systems and protocols to draw more focus to the consideration of cybersecurity during an exam. Specifically, the NAIC Financial Examination Handbook, which is used by insurance regulators as they examine insurers, incorporates the National Institute of Standards and Technology (NIST) concepts of Identify, Protect, Detect, Respond and Recover. It also incorporates improvements to encourage greater review and testing of cybersecurity exposure, as well as corresponding company controls, during the course of a financial examination. Other financial examination revisions include reviews of insurer cybersecurity training and education programs, incident response plans, understanding cybersecurity roles and responsibilities; post remediation analysis, consideration of third party venders, and how cybersecurity efforts are communicated to the board of directors. The NAIC is also in the process of updating our Market Regulation Handbook to strengthen sections regarding cybersecurity. Our Task Force also developed the Cybersecurity and Identity Theft Coverage Supplement for insurer financial statements to gather financial performance information about insurers writing cybersecurity coverage.[4]

The NAIC also continues to work toward developing an Insurance Data Security Model Law to establish standards for data security. The purpose and intent of the model law is to establish standards for data security, investigation, and notification of a breach applicable to insurance licensees and providing requirements for notifying regulators and consumers. It 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 are engaged with industry and consumer stakeholders as we continue the model's development, and look forward to sharing our progress with you.

We recognize that cybersecurity and associated regulatory concerns stretch beyond the insurance sector and we encourage coordination among financial regulators as we develop strategies to protect the financial infrastructure of this country.

Sincerely,

Ted Nickel
NAIC President
Commissioner
Wisconsin Office of the
Commissioner of Insurance

Julie Mix McPeak
NAIC President-Elect
Commissioner
Tennessee Department of
Commerce & Insurance

Eric A. Cioppa
NAIC Vice President
Superintendent
Maine Bureau of Insurance

David C. Mattax
NAIC Secretary-Treasurer
Commissioner of Insurance
Texas Department of Insurance

[3] Attachment B - NAIC *Roadmap for Consumer Cybersecurity Protections*, December 2015
[4] Attachment C - Report to the NAIC Cybersecurity Task Force on Cyber Supplement, August 2016

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

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/*

TO: Cybersecurity (EX) Task Force

FROM: Eric Nordman, CPCU, CIE, MCM
Director, Regulatory Services Division & the CIPR

Dan Daveline,
Director, Financial Regulatory Services Division

DATE: August 27, 2016

SUBJECT: Report on the Cybersecurity Insurance Coverage Supplement

The purpose of this report is to inform the Cybersecurity (EX) Task Force about the information filed by insurers in the Cybersecurity Insurance and Identity Theft Coverage Supplement (the Supplement) to the Property and Casualty Annual Statement for 2015. The report will also address some shortcomings in the data collection process and make some suggestions for future actions for the Task Force to consider.

Overview

Cybersecurity is crucial to effective and efficient operation of U.S. businesses. Cybersecurity breaches can cause a major drain on the U.S. economy. Insurers face cybersecurity risks in their daily operations as do banks and securities firms. The Financial Services Sector is perhaps the most under attack from cyber criminals. The reason for the attacks is multifaceted. Financial firms receive, maintain and store sensitive personal financial information from their customers. Insurers, in many cases, receive personal health information in addition to personal financial information. For insurers, information may be provided by policyholders or claimants. Cyber criminals are interested in this sensitive information as it can be used for financial gain by stealing a person's identity for fraudulent purposes. We know from observation of the dark web that personal health information is much more valuable these days than personal financial information. Nation states are also known to sponsor cyber-attacks for espionage or gaining access to corporate trade secrets and business processes.

Insurers are selling cyber risk management services and cybersecurity insurance products to businesses and individuals. It is to gain information and understanding about the cybersecurity insurance markets that led regulators to design and implement the Supplement. The first year the Supplement was required to be filed was with the 2015 Annual Statement filed in April of 2016. The data filed provides some interesting results. The initial results of these filings indicate over 500 insurers have provided businesses and individuals with cybersecurity insurance, with the vast majority of these coverages written as endorsements to commercial and personal policies. An overview shows a market of roughly $1.5 billion in direct written premium for insurers required to file the Supplement. Insurers writing standalone cybersecurity insurance products reported approximately $500 million in direct written premium and those writing cybersecurity insurance as part of a package policy reported roughly $ 1.0 billion in premium writings. The remainder of the report will provide figures filed for each category and explain assumptions used to arrive at the $ 1.5 billion in direct written premium. It will also discuss the entities reporting data and which entities might be missing from the data set. The report concludes with some recommendations for the Task Force to consider going forward.

Cybersecurity Insurance Coverage

The Supplement requires insurers to report the following information on standalone cybersecurity insurance policies:

- Number of claims reported (First Party & Third Party)
- Direct premiums written and earned
- Direct losses paid and incurred
- Adjusting and other expenses paid and incurred
- Defense and cost containment expenses paid and incurred
- Number of policies in-force (claims-made and occurrence)

The Supplement requires insurers to report the following information on cybersecurity insurance coverage sold as part of a package policy:

- Number of claims reported (First Party & Third Party)
- Direct premiums written and earned, if available or estimable
- Direct losses paid and incurred
- Adjusting and other expenses paid and incurred
- Defense and cost containment expenses paid and incurred
- Number of policies in-force (claims-made and occurrence)

Standalone Cybersecurity Insurance Policies

Perhaps the most interesting information is the size of the standalone cybersecurity insurance marketplace. Insurers writing this coverage reported $483,197,973 in direct written premium spread among 48 insurer groups (116 individual insurers). Direct earned premium reported was $373,742,189. Having less earned premium than written premium is indicative of a growing market. The top ten insurers wrote 78.7% of total U.S. market with the top 20 writing 95.8% of the market.

Loss ratios for standalone cybersecurity insurance were all over the map ranging from zero to over 500%. This too was not overly surprising. The market for cybersecurity insurance products is a new one and it is one with an element of catastrophe exposure. A zero loss ratio might be indicative of sound underwriting, but it might also simply be luck in selecting businesses that did not get hacked in 2015. The over 500% loss ratio occurred in an insurer group with less than $400,000 in direct written premium. Again, it could be indicative of poor underwriting or simply bad luck to insure a policyholder having a breach in 2015.

To keep things in perspective, the reader should remember $1.5 billion in direct written premium is only a very small percentage of the $522.4 billion in net written premium reported by the property and casualty insurers for 2015. All of these writings are supported by $703.6 billion in policyholder surplus held by insurers.

Package Policies

The reported direct written premium for cybersecurity package policies totaled $515,100,239. However, 257 insurers of the 574 insurers reported no premiums, generally because they could not break out the premium change for the cybersecurity coverage from the remainder of the package policy. To arrive at a figure representing a complete market NAIC staff assumed the 257 insurers writing cybersecurity package policies where premiums were not reported would have reported premiums in the same ratio as those insurers reporting actual premiums.

The actual mathematical calculation to extrapolate the premium dollars not reported under package policies follows:

- 257 insurers of 574 insurers reported no premium, representing 44.77% of the insurer population.
- The inverse of 44.77% is 55.23%.
- Then divide the actual package premium of $515,100,239 by 55.23% to get $932,645,734.
- As a result, by extrapolation we estimate approximately $933 million was the direct written premium sold through package policies.

Thus, we wish to inform you $1,415,843,707 is the reported and estimated total direct written premium for cybersecurity insurance coverage on a standalone and package policy basis for 2015.

Another interesting observation about the cybersecurity insurance policies sold on a standalone basis is most of the third party coverage is written on a claims-made basis. Approximately 82% of the policies were claims-made. From a solvency risk management perspective for insurers, the claims-made contract generally serves to limit exposure to the insurer compared to an occurrence policy by placing time limits on when the insured event must be reported to the insurer. While this is good for insurers, it is a coverage limitation from a policyholder perspective.

Identity Theft Coverage

From a market perspective, the year-end 2015 data clearly indicates that U.S. insurers' most common form of risk related to cybersecurity is in the form of identity theft coverage, where insurers wrote approximately 16.6 million policies including identity theft coverage as part of a package policy. This compares to only 496,000 policies that were stand-alone identity theft coverage.

From a risk perspective, the year-end 2015 data for identify theft coverage indicates the stand-alone premium on the 496,000 policies was $21.2 million, or approximately $42 per policy. Based upon this average of $42 per policy, the total amount of estimated annual premium on the 16.6 million policies with identify-theft as part of a package policy is still only approximately $700 million.

Caveats

When one uses data to gain information, it is important to understand its source, its attributes and its limitations. There are some important limitations for readers of this report to consider. The first limitation is the reported information is limited to only those insurers required to file a Property and Casualty Annual Statement with the NAIC. To evaluate this limitation, one must understand the types of insurers writing property and casualty business in the U.S. and whether each type is required to report information to U.S. regulators. With apologies to regulators who already understand what is said in this section, we believe it is important for readers not completely familiar with the U.S. regulatory framework to understand, from a state insurance regulators' perspective, the admitted and surplus lines markets.

The U.S. regulatory system for property and casualty insurance views insurers as belonging in one of three classifications. They are: domestic, foreign and alien. A domestic insurer is one

licensed or admitted in a state it selects to be its home state. A foreign insurer would be one licensed or admitted in a state that is domiciled in another state. An alien insurer is one domiciled in another country. Generally states insist insurers be licensed or admitted in the state as a prerequisite for selling property and casualty insurance products. However, state legislatures recognize not every person or business seeking coverage for unique risks can find it from a licensed or admitted insurer. Thus, state legislatures have allowed non-licensed insurers to write property and casualty business under certain circumstances. The insurers doing business as non-licensed or non-admitted insurers are known as surplus lines insurers. They serve as an alternative marketplace to provide coverage for unique exposures and often serve as a testing ground for product innovations before they become mainstream. Such is the case for cybersecurity insurance products. Offering coverage on a surplus lines basis allows the insurer greater freedom in pricing and does not require formal prior approval of contract language.

If an insurer is licensed or admitted in one or more states, it is required to submit an Annual Financial Statement, including the Supplement. Thus, all domestic and foreign insurers are required to file the Supplement as they will be considered an admitted insurer in at least one state. Alien insurers can choose to be licensed or admitted in one or more states if they wish. If they do choose to be licensed or admitted, then they too must file the Supplement. However, if an alien insurer decides not to become licensed in any state, the District of Columbia or U.S. territory, then no Supplement filing is required. The premium writings by alien surplus lines insurers are missing from the information contained in this report. Since we believe there may be a significant amount of premium written by alien surplus lines insurers, the reader should be cognizant of this potentially important missing element.

What Others are Saying about the Cybersecurity Insurance Markets

"Cyber coverage is the fastest growing surplus lines business in history and it was caused by a regulation, not by some other market factor. It's a $1 billion line right now."—Benjamin J. McKay, Executive Director of the Surplus Line Association of California

"The cyber insurance marketplace has grown to over $2 billion in gross written premiums with industry prognosticators forecasting it to double by 2020. The number of carriers offering cyber insurance has increased following a spate of cyberattacks that have brought the potential and need for such insurance into sharper focus."—PartnerRe

"We expect worldwide spending on Cybersecurity products and services to eclipse $1 trillion for the five-year period from 2017 to 2021"—Steve Morgan, Founder and Editor-In-Chief at Cybersecurity Ventures

"Cyber insurance is a potentially huge, but still largely untapped, opportunity for insurers and reinsurers. We estimate that annual gross written premiums are set to increase from around $2.5 billion today to reach $7.5 billion by the end of the decade."—PwC Report—Insurance 2020 & beyond: Reaping the dividends of cyber resilience

"Annual premium volume information about the U.S. cyber-risk market is hard to come by, but in reviewing the market, we have concluded that the annual gross written premium may be as much as $3.25 billion (up from $2.75 billion in last year's report)."— Richard S. Betterley, CMC, President, Betterley Risk Consultants, Inc. from Cyber/Privacy Insurance Market Survey—2016

"The cyber market is growing by double-digit figures year-on-year, and could reach $20 billion or more in the next 10 years. …fewer than 10% of companies are thought to purchase cyber insurance today."—Nigel Pearson, Global Head of Fidelity, Allianz Global Corporate & Specialty

Recommendations for the Task Force

A major caveat contained in this report is the missing information on the amount of premium written by alien surplus lines insurers. Staff believes there may be significant premium writings, particularly for standalone cybersecurity insurance policies, in this segment of the overall markets. Staff recommends the Task Force consider approaching the Surplus Lines (C) Task Force to request making submission of some or all of the information contained in the Supplement a condition for continuing to be listed on the *Quarterly Listing of Alien Insurers*.

A second staff recommendation is for the Task Force to take comments from interested parties on how the instructions or the format of the Supplement could be improved.

Conclusion

While the first report of any data collection exercise is challenging, the quality of the data improves with subsequent filings. This report summarizes some interesting findings. If information can be obtained from the alien surplus lines insurers, a more complete picture of the 56 U.S. cybersecurity insurance markets will emerge. Having a time series will allow regulators to track market growth and pinpoint areas where further regulatory oversight is needed.