April 16, 2019

Director Bruce R. Ramge, Chair
Market Conduct Examination Standards (D) Working Group
NAIC Central Office
1100 Walnut, Suite 1500
Kansas City, MO 64106-2197

Attn: Petra Wallace, Market Regulation Specialist

VIA Electronic Mail: pwallace@naic.org

RE: Insurance Data Security Pre- and Post - Breach Checklists for Inclusion in the Market Regulation Handbook

Dear Director Ramge:

The American Property Casualty Insurance Association (APCIA)[1] appreciates the opportunity to provide supplemental comments on the National Association of Insurance Commissioners' (NAIC) draft Insurance Data Security Pre- & Post-Breach Checklists (Checklists) for inclusion in the Market Regulation Handbook (Handbook). As follow-up to the APCIA letter dated March 6th, 2019, we offer additional suggestions below for the Checklists' Overview and Guidelines. The recommendations are intended to (1) clearly identify when the pre-breach checklist should be utilized; (2) further emphasize the need for consultation with domestic financial examiners to leverage the IT examination; and (3) highlight that the data security model is risk-based and that a risk-based analysis will underlie all decisions made by Licensees. Much of the risk-based language is borrowed from the IT Examination Handbook.

APCIA Recommended Edits

Note: The guidance that follows should only be used in states that have enacted the *NAIC Insurance Data Security Model Law (#668)* or legislation which is substantially similar to the model. Moreover, in performing work during an exam in relation to the Model Law, it is important the examiners first obtain an understanding and leverage the work performed by other units in the department and, to the extent possible and preserving the confidentiality and security of the information, at the domiciliary regulator including but not limited to financial examination-related work.

Importantly, examiners must also recognize that the Model Law and implementation of security measures is risk-based and should be mindful that the insurer is not required to include all of the components of the Model Law or any single or particular information technology security framework as part of its Information Security Program. An Information Security Program is instituted based on an insurer's risk exposure, which

[1] Representing nearly 60 percent of the U.S. property casualty insurance market, the American Property Casualty Insurance Association (APCIA) promotes and protects the viability of private competition for the benefit of consumers and insurers. APCIA represents the broadest cross-section of home, auto, and business insurers of any national trade association. APCIA members represent all sizes, structures, and regions, which protect families, communities, and businesses in the U.S. and across the globe.

may vary based on, for example, volume, type of sensitive information and the broad security environment in which the insurer is operating. There are many factors that will influence the policies and programs and the security framework or frameworks that are appropriate for a particular insurer to effectively protect is sensitive information and information technology structure.

OVERVIEW

The purpose and intent of the Insurance Data Security Model Law is to establish standards for data security and standards for the investigation of and notification to the Commissioner or Director of Insurance of a Cybersecurity Event affecting Licensees.

REVIEW GUIDELINES AND INSTRUCTIONS

When reviewing a Licensee's Information Security Program for compliance with the Insurance Data Security Model Law (NAIC Model #668) for the prevention of a Cybersecurity Event as defined in the model law, please refer to the examination checklist attached as Exhibit A hereto. When a specific need arises to utilize the pre-breach checklist, coordination with other units in the department and, to the extent possible, at the domiciliary regulator is critical to promoting efficiency and resiliency.

When reviewing a Licensee's Information Security Program and response to a Cybersecurity Event for compliance with the Insurance Data Security Model Law subsequent to a suspected and/or known Cybersecurity Event as defined in the model law, please refer to both examination checklists attached as Exhibits A and Exhibit B hereto.

When considering whether to undertake such a review, refer to Section 9 of NAIC Model #668, which provides certain exceptions to compliance for Licensees with fewer than ten employees; Licensees subject to the Health Insurance Portability and Accountability Act (Pub.L, 104-191, 110 Stat. 1936, enacted August 21, 1996);

Additional Checklist Amendments

Upon further review of the Checklist we highlight at least two additional considerations for the Working Group. First, should questions 9 and 15 in the Pre-Breach Checklist be combined? These two questions seem slightly redundant. Second, Section 4(E) indicates that the executive management can *delegate* development, implementation, and maintenance of an ISP and if executive management does delegate these responsibilities its job is then one of oversight. As such, we recommend Question 3 read: "Has the ISP been reviewed and approved by the Licensee's executive management or its delegates."

****

Thank you for your continued collaboration. If you have any questions or would like to discuss any of these recommendations further, please let us know.

Respectfully submitted,

Angela Gleason and Alex Hageli

