
*Roberta Meyer*
*Vice President & Associate General Counsel*

December 18, 2018

Director Bruce R. Ramge, Chair
Mr. Jim Mealer, Vice Chair
Market Conduct Examinations Standards (D) Working Group
National Association of Insurance Commissioners
1100 Walnut Street, Suite 1500
Kansas City, MO 64106

Attn: Petra Wallace

Via e-mail: pwallace@naic.org

Re: Insurance Data Security Pre-Breach and Post-Breach Checklists – 12-17-18 Revised Draft

Dear Director Ramge and Mr. Mealer:

The American Council of Life Insurers (ACLI)[1] thanks the Market Conduct Examination Standards (D) Working Group (Working Group) for its continuing discussion of the Insurance Data Security Pre-Breach and Post-Breach Checklists (Checklists), proposed to be included in the Market Regulation Handbook (Handbook) and the opportunity to submit comments on the most recent (12/17/18) draft of the Checklists.

ACLI appreciates the inclusion of the Note at the beginning of the Checklists that provides that the following guidance should only be used in states that have adopted the NAIC Insurance Data Security Model Law (Model Law) or substantially similar legislation and that it is important examiners obtain an understanding and leverage the work performed by other units of the department.

As discussed during the 11/29/18 Working Group call, ACLI recognizes it is not the purpose of the Handbook to specify how jurisdictions allocate market and financial regulation staff when conducting an insurance data security exam. At the same time, ACLI respectfully submits that performance of pre-beach assessments solely as part of financial examinations will further insurers' resiliency, provide for examinations by individuals likely to have more appropriate expertise for assessing insurers' information security systems, promote efficiency and avoid duplication of work and inconsistent application of examination standards. Accordingly,

[1] The ACLI advocates on behalf of 290 member companies dedicated to providing products and services that promote consumers' financial and retirement security. Ninety million families depend on our members for life insurance, annuities, retirement plans, long-term care insurance, disability income insurance, reinsurance, dental, visions and other supplemental benefits. ACLI represents member companies in state, federal, and international forums for public policy that supports the industry marketplace and the families that rely on life insurers' products for peace of mind. ACLI members represent 95 percent of industry assets in the United States.



 

ACLI respectfully urges the Working Group not to recommend inclusion of a pre-breach checklist in the Handbook for use as part of a market conduct exam.

If the Working Group determines the above is not possible, in line with discussion during the 11/29/18 Working Group call, ACLI urges modification to the current (12/17/18) draft of the Checklists to provide for the Handbook to: (i) incorporate a post-breach checklist only; and (ii) make any pre-breach guidance available in the Handbook reference documents.

If a pre-breach checklist is provided in the Handbook or its reference documents, ACLI urges that it be preceded by a reminder to examiners that the Model Law specifies that its requirements are to be based on a licensee's risk profile and that insurers' data security systems are to be risk-based.

Further, in line with other comments submitted to the Working Group, ACLI is concerned that a number of the criteria in both the pre-breach checklist and the post-breach checklist are not in the Model Law or deviate from the corresponding provisions of the Model Law.

For example, and of particular concern:

(i) Criteria 3, 4, and 5 in the pre-breach checklist, appear to require multiple levels of review of an insurer's security program in contrast with the Model Law's requirement that the Licensee's executive management or its delegates develop, implement and maintain the Licensee's data security program;

(ii) Criteria 31 in the pre-breach checklist appears to require an insurer's incident response program to provide detailed instructions for internal and external communications, as well as information sharing with regulatory authorities, which may be construed to have an extraterritorial effect, while the Model Law has no such requirements;

(iii) Criteria 2, 5, and 6 in the post-breach checklist respectively inquire if the licensee *appropriately* determined the nature and scope of the breach, provided *timely* updates to the initial and other required notifications, and provided *timely and sufficient* notice of the Cybersecurity Event to consumers *(Italics added),* using troubling subjective language, not in the Model Law, that could be subject to different interpretations.

(iv) Criteria 8 in the post-breach checklist also provides for a subjective interpretation by inquiring if the Licensee provided *timely and sufficient* notice to independent insurance producers and/or producers of record while the Model Law only requires provision of notice to independent producers under specified circumstances.

ACLI respectfully urges modification to any criteria included in any pre or post breach checklist included in the Handbook or any reference documents of the Handbook to track the language of the Model Law to the greatest extent possible.

ACLI appreciates and thanks the Working Group for its consideration of our concerns, and would be glad to answer questions relating to any of the above.

Sincerely,

Robbie Meyer

G:\MKTREG\DATA\D Working Groups\D WG 2018 MCES (PCW)\Docs_WG Calls 2018\Ins Data Security\Comments Received\ACLI 12-18-18 Comments.docx



 