July 24, 2026

Chair Brett Bache
Vice Chair Danielle Torres
NAIC Market Conduct Examination Guidelines (D) Working Group
1100 Walnut Street
Suite 1000
Kansas City, MO 64106-2197

Sent via: pwallace@naic.org

Dear Chair Bache, Vice Chair Torres, and Market Conduct Examination Guidelines (D) Working Group Members,

Thank you for the opportunity to provide comments on the Market Conduct Examination Guidelines Cybersecurity Event Response Coordination Framework. We appreciate the opportunity to provide feedback, noting the importance of continued communication and collaboration across the overlapping H Committee workstreams. At this point in time, we have questions surrounding the scope and intention of this framework, mainly whether this is intended to provide efficiency in reporting and regulator incident reporting frameworks. Further, it would be important to understand and include any information on how this framework fits with the Cybersecurity (H) Working Group's Cybersecurity Event Portal project timewise. Without a more coherent understanding of how this framework would harmonize with existing reporting frameworks, we do not encourage this working group to adopt an additional layer to an already complicated regulatory reporting scheme.

Further, absent a thorough analysis of the risks of potentially reporting and maintaining this sensitive information in one place (with access across many states), we have concerns with how this information would remain adequately protected. A deeper understanding of what is envisioned by this framework would be beneficial from a confidentiality and data security standpoint. We hope to engage in further dialogue with this Working Group and are readily available to provide any follow-up information.

IDSM Adoption & Appropriate Oversight

- ACLI members have a preference for working with their current regulators who have the authority and access to their cybersecurity incident information (lead states, other states that have adopted the Insurance Data Security Model #668 ("IDSM")). *These current reporting systems are known to member companies and allow for the most efficient response times*, something which could be confused or overly complicated by a framework such as the one suggested here which could inadvertently create a "51st state." This concern with an additional oversight regime is complicated by the potential for states without authority over a company to have the ability to see breach or incident information via the NAIC.
    - There is also a concern with states initiating exams based on information learned through this framework despite lacking the authority to open an exam. If adopted, it would be important to include language in the Scope section as to the intended uses and by whom.

- The existing framework language seems to conflict with the IDSM, giving NAIC authority to determine whether a particular cybersecurity event would require additional regulator engagement. The framework appears to be inconsistent with reporting processes today where companies notify regulators consistent with either the IDSM, specific NYDFS regulations, or other relevant laws in other states. A better understanding of the expansion of authority in this framework would assist in providing further comments.
- This framework attempts to simplify the current complicated incident reporting process that, if all states adopted the IDSM, might serve to abridge current complex reporting and regulator incident analysis. However, there is not a majority of states that have adopted the IDSM to date, and adopting this framework would create an additional regulatory layer. *We once again advocate for further adoption of the IDSM in states that have not adopted the IDSM*, with the potential to adopt a framework like this at that time when there are a significant number of states with more uniform regulations and laws.
    - Existing incident response requirements are layered by complexity even beyond the difference between IDSM reporting states and states who have not adopted the IDSM. Materiality thresholds, number of impacted consumer thresholds, and reporting to a state Attorney General versus Insurance Commissioner all differ state to state. For some carriers that fall under HIPAA reporting requirements for covered entities, there is an additional federal layer on top of the complex state reporting. Lastly, the actual information being reported differs depending on the jurisdiction or impacted consumers, leading to a patchwork regulatory scheme that does not appear to be alleviated by the proposed framework, but rather further exacerbated.
- The catch-all provision that "any situation in which regulators deem that this Framework would benefit the work of state insurance regulators" would fall within scope, effectively removes any meaningful activation threshold. The criteria should include a defined minimum (e.g., number of affected states or policyholders, demonstrated cross-jurisdictional impact) to keep the framework reserved for events of genuine and material significance.
- Lastly, there is further scope ambiguity due to no referenced definition for "cybersecurity event" in the framework. Would the IDSM definition be the point of reference for this framework? Absent a definition of event or a reference to a definition, there are questions as to the types of events regulators will consider in scope.

Lead State Coordination

- If explored further, the framework should be more explicit that the Lead State is the primary regulatory point of contact with the affected insurer during activation, and that participating states ordinarily channel requests through the Lead State rather than reaching out independently. Without that clarity, there is a risk of adding a coordination layer on top of existing multi-state demands rather than meaningfully reducing them.
- At present, the framework does not address how confidential information shared by the regulated entity will be protected as it moves from the Lead State to participating states and NAIC staff. Clarification that information shared under the framework will be handled consistent with applicable confidentiality protections under Model #668 and relevant state examination or investigative confidentiality laws, including appropriate limits on further disclosure, would be beneficial.
- Section 4 appears to grant the Lead State responsibility for determining whether violations occurred and what corrective action is appropriate. However, the framework does not address how participating states would concur in or adopt those findings, whether those findings are binding, or what happens when states disagree. Without that clarity, a company could face a Lead

State finding plus independent enforcement from non-concurring states. The framework should address the intended effect of Lead State determinations on other states' enforcement authority.
- The framework does not address harmonization with existing breach-notification timelines (e.g., the 72-hour requirement under Model #668), ongoing state examinations, or parallel federal and law-enforcement investigations. Clarification that activation does not itself create new or accelerated notification obligations beyond those imposed by applicable law and how the Lead State and participating states are expected to coordinate with other regulators and law-enforcement authorities to minimize conflicting or duplicative directives, would provide more clarity.

Market Conduct Examinations & Post-Incident Time Allocation

- The time it would take to execute this framework seems to conflict with the time it takes affected states to address the event and its impact. Instead of mitigating potential damage across the industry in the wake of a cybersecurity event, this framework creates a complicated tool which could be punitive in nature and hinder the ability of impacted states and consumers to receive the most timely and efficient information.
- Further, the timing of a post-incident report with a potentially simultaneous market conduct exam, does not appear to enhance the goals of efficiency and consumer protection.
    - Beginning a market conduct exam simultaneously with assessing resolution or remediation of the event seems overly burdensome, premature, and harmful.
- The draft appears to presume that a market conduct or financial exam automatically follows a cybersecurity event when such an exam is not currently a foregone conclusion and may not be appropriate or warranted. In particular, the Cybersecurity Coordination Framework- Illustrative seems to assume an exam will take place. If this is not the intention of the framework, a better understanding of scope and the relationship and harmony with existing incident reporting and exam frameworks would be helpful.
- There are remaining questions around the purpose and ultimate goal of the framework alongside other NAIC workstreams. Will this coordination framework connect to a reporting framework (i.e. the Cybersecurity Event Portal)?
    - If the intention is to complement the Event Portal, we would feel more comfortable considering the framework in the context of a finalized portal. If the intention is to start with the framework as opposed to a state's individual assessment of whether or not to conduct a market conduct exam, we would have concerns as to the purpose and lack of efficiency in this endeavor.
- Given the uncertainty in the current framework's objective, there is also a concern with whether this would encourage automatic inquiries to companies in the wake of national cybersecurity incidents, regardless of whether the company did experience impact. This type of immediate inquiry not only diverts time and resources of company departments that are potentially not impacted by a breach, but also can lead to unwarranted or questionable data calls based on unconfirmed assumptions.

Confidentiality & Preliminary Assessment Questions

- Given the sensitivity of exposing specific vulnerabilities/weaknesses a company had in the cybersecurity or privacy space, would any reports or consent orders be handled differently than standard exam reports in terms of publication? There are significant concerns around the confidentiality of information shared and how access to that information will be properly limited to *only* those with the authority to review the company's reporting.
- How would access and sharing be handled confidentially among states?
- How would information be limited to *only* impacted states or states that follow the IDSM?

- What would the preliminary assessment look like to determine the treatment of an inquiry versus an industry event? This information would be helpful in considering the necessity of a framework.
- Will there be mandatory requests that companies must respond to in order to identify if further action is necessary?
- Would these communications happen simultaneously with other inquiries and reporting obligations in non-IDSM states in the wake of a cybersecurity event?
- What entity would create a portal or other access point for the various involved states (where would information be stored)?

Overall, we appreciate the opportunity to provide feedback, however the timing of this framework prior to the creation of a Cybersecurity Event Portal, the lack of substantial IDSM adoption across states, the potential vulnerability and risk of this type of framework, and the timing aspect of this framework following an incident and predating or coinciding with a potential exam, all create burdens that could outweigh the benefits of this added layer of oversight. More context and opportunities for stakeholder input would allow us to provide more tailored feedback and redlines moving forward. We are happy to provide any follow-up to our comments.

Thank you,

Kirsten Wolfford
Associate General Counsel
ACLI
kirstenwolfford@acli.com

