WASHINGTON, DC • LONDON • BRUSSELS • HONG KONG • WWW.ICI.ORG

December 22, 2022

Secretariat to the Financial Stability Board
c/o Bank for International Settlements
Centralbahnplatz 2
CH-4002 Basel
Switzerland
Submitted electronically to: fsb@fsb.org

RE: FSB Consultative Document on Achieving Greater Convergence in Cyber Incident Reporting

Dear Sir or Madam,

The Investment Company Institute (ICI), including ICI Global[1], appreciates the opportunity to comment on the Financial Stability Board's (FSB) consultative document on Achieving Greater Convergence in Cyber Incident Reporting.[2]

The importance of, and necessity for, effective information security increases with each passing day as bad actors remain intent on penetrating systems of financial institutions to access or exfiltrate their data. ICI's members have long taken seriously their obligation to protect their systems and the confidentiality of their non-public information against any type of threat – including cybersecurity threats. This is not surprising as our members' brands and success as a business are highly dependent upon investor confidence.

We offer the following comments in response to the FSB's consultative document and to the questions outlined in the FSB's invitation for feedback.

Challenges to achieving greater convergence in Cyber Incident Reporting (Section 2)

We agree with the emphasis in the consultation paper on focusing on practical issues related to Cyber Incident Reporting (CIR), as the need to overcome practical and operational challenges is consistent with the experience of ICI's members.

An asset management firm with global operations will have many regulatory reporting requirements across all of the jurisdictions in which it operates. These requirements are not homogenous, and while each individual regulatory requirement's goal is to improve resilience, the actual result can be a degradation of resilience via a drain on resources at the very moment these resources are needed to combat a significant cyber incident.

---

[1] ICI Global carries out the international work of the Investment Company Institute, the leading association representing regulated investment funds. With total assets of $35.2 trillion, ICI's membership includes mutual funds, exchange-traded funds (ETFs), closed-end funds, and unit investment trusts (UITs) in the United States, and UCITS and similar funds offered to investors in Europe, Asia and other jurisdictions. ICI's mission is to strengthen the foundation of the asset management industry for the ultimate benefit of the long-term individual investor. ICI Global has offices in Brussels, London, Hong Kong, and Washington, DC.

[2] https://www.fsb.org/2022/10/fsb-makes-proposals-to-achieve-greater-convergence-in-cyber-incident-reporting/

FSB recommendations to address impediments to achieving greater convergence in CIR (Section 3)

In response to the recommendations contained in Section 3 of the consultative document we offer the following comments and observations.

In order to ensure that a regulator receives notice of those incidents of greatest concern to registrants, regulators, and potentially financial markets, we would recommend clarifying and narrowing the scope and terminology related to CIR. For the purposes of effective CIR, a cyber incident should be defined as a 'significant cybersecurity incident,' meaning an incident or group of incidents that significantly disrupts or degrades a financial institution's (FI) ability to maintain critical operations or leads to the unauthorized access or use of information where such unauthorized access or use results in substantial harm to the FI or the investor whose information was accessed.

By appropriately defining and narrowing the scope of cyber incidents for reporting, it will help to filter out the noise of other cyber incidents that do not significantly impair FI operations, information, or systems, while focusing on providing alerts and reports of disruptions in critical operations or substantial harm to an FI or investors.

We support the recommendation for a phased approach to reporting (Recommendation 4) as a pragmatic approach, which is aligned with how actual events unfold during a significant cyber incident and the information that is typically available to report over different times and phases of the incident.

Regarding the triggers and reporting windows (Recommendations 5 and 6), we recommend that the impetus for the initial report should be based on an FI having definitively concluded that a cyber incident is occurring or has occurred rather than being based on an arbitrary time period. The expectations from the relevant authorities for such reporting should also take into consideration that information at an early juncture may necessarily be incomplete and that whatever information is submitted in the initial CIR is subject to change as additional information regarding the incident becomes available.

We concur with the importance of protecting sensitive information as part of the CIR process (Recommendation 16). Further, we would underscore the importance that CIR by FIs to the relevant authorities must take place via an 'out of band' channel or network in cases when an FI's network is potentially compromised. There have been numerous publicly reported instances in which an attacker compromised a victim's network, and the victim subsequently engaged in communications with external parties about the response to the attack, without realizing that the attacker was able to monitor these communications. Early in the reporting cycle, it may not be feasible to communicate disclosures using normal channels if those communication channels are potentially compromised. To address this challenge, the relevant authorities should have systems in place in advance to accommodate this situation.

We also note that the need to protect sensitive information as outlined in Recommendation 16 is also relevant to any cross-border or sectoral information sharing (Recommendations 11 and 15). While we acknowledge the potential benefits of information sharing to bolster response and defensive capabilities, it is critical that any information sharing include a central role for data protections, with well-articulated and verified controls regarding transmission protocols, data storage, and confidentiality. Without such controls in place CIR data could itself become a target for potential attacks and further breaches.

Format for Incident Reporting Exchange (FIRE) (Section 5)

The FIRE concept is attractive, as a harmonized central incident reporting format could help to address some of the practical and administrative challenges inherent in CIR for FIs operating in multiple jurisdictions.

However, additional information and clarification would be helpful in several areas, some of which have also been appropriately highlighted in the FSB consultative document.

- First, it is unclear what entity will be responsible for ongoing development and maintenance of FIRE in response to continued developments in the sector and evolving trends.
- Second, it would be helpful if FIRE also specified the security protocols necessary for implementation, including the security of the data at rest, in motion, and by the recipient.
- Third, if FIRE moves forward, it would be helpful for some entity to maintain a dynamic list of which regulators and relevant authorities have adopted FIRE.
- Finally, given the important role of third-party service providers in supporting the asset management industry and broader financial sector, we would suggest that critical third parties be included in developing the FIRE concept.

Thank you again for the opportunity to provide feedback on this issue. We welcome continuing the dialogue which will be essential to developing convergence in CIR. If you have any questions, please contact me at michael.pedroni@ici.org or +1-202-853-2186 or Peter Salmon at salmon@ici.org or +1-202-326-5869.

Sincerely,
/s/ Michael Pedroni

Michael N. Pedroni
Chief Global Affairs Officer and Head of ICI Global
Investment Company Institute