December 19, 2024

Via Electronic Mail

Mr. John Schindler
Secretary General
Financial Stability Board
Bank for International Settlements
Centralbahnplatz 2
CH-4002 Basel
Switzerland

Re: Format for Incident Reporting Exchange (FIRE)—Consultation Report

Dear Mr. Schindler,

The Bank Policy Institute ("BPI")|BITS[1], appreciates the opportunity to comment on the Financial Stability Board's Format for Incident Reporting Exchange ("FIRE") consultation.[2] Overlapping and duplicative regulatory requirements continue to consume finite cyber resources for financial institutions—with varying cyber incident reporting obligations presenting particular operational challenges. The FSB's work to promote convergence between incident reporting requirements will help financial institutions more effectively coordinate incident response efforts and better manage financial stability risks.

In the United States alone, financial institutions have as many as ten distinct Federal cyber incident reporting requirements.[3] This does not account for additional reporting requirements at the state level, like notifying the New York Department of Financial Services. Many of these regulatory obligations have different thresholds for reporting, notification timelines, and information requirements. Those differences require front-line cyber personnel to spend more time on compliance activities leaving less time to mitigate incident impacts.

[1] The Bank Policy Institute is a nonpartisan public policy, research and advocacy group that represents universal banks, regional banks, and the major foreign banks doing business in the United States. The Institute produces academic research and analysis on regulatory and monetary policy topics, analyzes and comments on proposed regulations, and represents the financial services industry with respect to cybersecurity, fraud, and other information security issues. Business, Innovation, Technology and Security ("BITS"), BPI's technology policy division, provides an executive-level forum to discuss and promote current and emerging technology, foster innovation, reduce fraud, and improve cybersecurity and risk management practices for the financial sector.

[2] FIN. STABILITY BD., FORMAT FOR INCIDENT REPORTING EXCHANGE (FIRE): CONSULTATION REPORT 1 (2024).

[3] DEP'T OF HOMELAND SEC., HARMONIZATION OF CYBER INCIDENT REPORTING TO THE FEDERAL GOVERNMENT 9 (2023); U.S. DEP'T OF HOUSING & URBAN DEVELOPMENT, FED. HOUSING ADMIN., MORTGAGEE LETTER 2024-10, SIGNIFICANT CYBERSECURITY INCIDENT (CYBER INCIDENT) REPORTING REQUIREMENTS (2024); U.S. DEP'T OF HOUSING & URBAN DEVELOPMENT, GINNIE MAE, APM 24-02, CYBERSECURITY INCIDENT NOTIFICATION REQUIREMENT (2024).

While not the exclusive cause, the recent proliferation of cyber incident reporting requirements globally has at least partially contributed to the operational challenges facing financial institutions—especially during the early stages of responding to an incident. Based on a recent survey of our member firms, financial institutions reported their cyber teams now spend more than 70 percent of their time on regulatory compliance activities. Those same firms reported that their Chief Information Security Officers or comparable senior cyber leaders spend between 30 to 50 percent of their time on those same regulatory compliance matters.

Given the complex financial regulatory landscape, BPI welcomes the FSB's efforts to develop a framework that promotes uniformity across global incident reporting requirements. To help FIRE achieve its stated objective, we recommend that the FSB encourage regulators to: (1) only require reporting for material incidents that cause actual harm; (2) not require additional data elements for reporting beyond those proposed in FIRE; and (3) preserve the security and confidentiality of reported information.

I. Limit Reporting to Incidents Causing Actual Harm

The FSB's consultation proposes common elements for incident reporting including information on the entity providing the report, incident details, an impact assessment, and remedial actions taken.[4] Collectively, these categories would provide regulators with the information they need to understand an incident's impact and any additional measures necessary to prevent further harm.

At the same time, the FSB does not discuss at length materiality thresholds for incident reporting. Discussion of this topic is critical because conflicting thresholds for incident reporting remain a key impediment to harmonizing regulatory requirements globally. Consequently, we suggest that the FSB recommend that regulators limit the scope of reporting to incidents causing actual harm or substantially impacting a critical portion of a company's business. Tailoring requirements in this way will limit overreporting on inconsequential events that do little to inform cyber risk oversight.

II. Regulators Should Not Require Data Elements Beyond Those Proposed in FIRE and Existing Legal Authorities

The FSB's consultation outlines 99 data elements for incident reporting—51 of which are optional.[5] This provides regulators with flexibility to implement FIRE in a way that satisfies their unique oversight needs. Importantly, the FSB reminds regulators to remain "mindful not to compound operational challenges" when selecting data elements for incident reporting.[6]

To the extent that regulatory agencies adopt FIRE, it is important that they do not use the template as a "floor" for incident reporting and simply add additional requirements beyond those proposed by the FSB. Such an approach would forfeit any convergent benefits FIRE might hope to achieve.

Similarly, when selecting data elements for incident reporting, regulators should be careful to only mandate items consistent with their authorities and directly related to some actionable purpose.

---

[4] FIN. STABILITY BD., FORMAT FOR INCIDENT REPORTING EXCHANGE (FIRE): CONSULTATION REPORT 9 (2024).
[5] *Id.* at 1.
[6] *Id.*

When an incident is first identified, front-line cyber personnel need sufficient time to investigate without their limited bandwidth being entirely consumed by compliance obligations. Regulators need to receive timely notification of incidents to understand their implications and warn similarly situated entities. Nonetheless, regulators should be cognizant of the information they are requiring from impacted entities during an incident and be careful to ensure that compiling that data will not create more burden than any benefit regulators can derive from that information.

III. Preserve the Security and Confidentiality of Reported Information

When complying with the various financial sector incident reporting requirements, firms provide regulators with sensitive information, which, if exposed, could further damage impacted entities. Moreover, because reported information is often aggregated within regulatory agencies, the systems housing that data become attractive targets for cyber adversaries. This risk is particularly acute for impacted entities who have not fully remediated an incident at the time they submit their first report.

Recognizing these risks, BPI suggests that the FSB include guidance to regulators expressing the importance of applying appropriate security measures that preserve the confidentiality of reported information. To inform that guidance, the FSB could reference the requirements codified in the Cyber Incident Reporting for Critical Infrastructure Act ("CIRCIA") requiring U.S. Federal agencies to provide appropriate protections for information submitted by private sector companies.[7] Among other things, these requirements mandate that personal information be protected from unauthorized use or disclosure and that reported information be "collected, stored, and protected at a minimum in accordance with the requirements for moderate impact Federal information systems" under Federal Information Processing Standards Publication 199.[8] The FSB might also consider recommending additional protections in CIRCIA that would: (1) bar reported information from being used in regulatory enforcement actions; (2) preserve attorney-client privilege; and (3) prohibit reported information from being received in evidence or otherwise subject to discovery.[9]

In addition, BPI suggests that the FSB exclude data fields for reporting on sensitive information that could create legal exposure for firms. Information related to legal and regulatory impacts[10]—when combined with data on vulnerabilities exploited during an incident—is an example of one such data field. Incident reports are commonly shared across authorities within a jurisdiction and firms often do not have visibility into which regulatory agencies ultimately have access to the incident reports they submit. Therefore, BPI recommends that FSB strike reporting on an incident's legal or regulatory impact.

IV. Conclusion

A balanced approach to cyber incident reporting is pivotal to promoting the efficient and effective response processes necessary to mitigate financial stability risks. BPI would welcome the opportunity to work collaboratively with the FSB to achieve that desired outcome. If you have any questions or would like to discuss these comments further, please contact Patrick Warren at patrick.warren@bpi.com.

[7] 6 U.S.C. § 681e.
[8] *Id.*
[9] *Id.*
[10] FIN. STABILITY BD., FORMAT FOR INCIDENT REPORTING EXCHANGE (FIRE): CONSULTATION REPORT 39 (2024).

Sincerely,

/s/ Patrick Warren
Patrick Warren
Vice President, Regulatory Technology
BITS, Bank Policy Institute