Martin Boer
Senior Director
Regulatory Affairs

December 19th, 2024

Mr. John Schindler
Secretary General
Financial Stability Board (FSB)
Bank for International Settlements
Centralbahnplatz 2
CH-4002 Basel, Switzerland
(Submitted electronically)

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

Dear Mr. Schindler,

The Institute of International Finance (IIF)[1] and its members are pleased to respond to the Financial Stability Board (FSB) Format for Incident Reporting Exchange (FIRE) Consultation Report."[2] We recognize and appreciate the FSB's long-standing leadership in addressing market fragmentation and encouraging coordination, consistency and cooperation among its member jurisdictions, and with other global standard-setting bodies.

We also commend the FSB for its critical work in promoting greater harmonization around cyber security and cyber risk practices, including in this case around incident reporting across financial institutions and reporting authorities around the world.

The importance of effective cyber incident reporting

Cyber incident reporting (CIR), when used effectively, can be a beneficial tool that helps protect individual financial services firms, the financial sector, and the global financial system. Increased cyber threat and incident awareness, visibility, and information exchange, including across jurisdictions and public and private sector entities, can help disrupt and stop adversaries and assist affected financial institutions (FIs) with protection, mitigation, and response. The proliferation of cyber incidents in recent years has only highlighted the importance of coordinated

[1] The Institute of International Finance (IIF) is the global association of the financial industry, with about 400 members from more than 60 countries. The IIF provides its members with innovative research, unparalleled global advocacy, and access to leading industry events that leverage its influential network. Its mission is to support the financial industry in the prudent management of risks; to develop sound industry practices; and to advocate for regulatory, financial, and economic policies that are in the broad interests of its members and foster global financial stability and sustainable economic growth. IIF members include commercial and investment banks, asset managers, insurance companies, professional services firms, exchanges, sovereign wealth funds, hedge funds, central banks, and development banks.
[2] FSB 2024. "Format for Incident Reporting Exchange (FIRE) Consultation Report" October 17, 2024.

information sharing that is calibrated properly, and that reporting regimes should be streamlined and effective to support the number of cyber incidents.

Effective incident response and recovery is also essential to help mitigate shocks to financial stability. Given that adversaries usually attack multiple institutions simultaneously, and often do so across borders, it is imperative that critical information, including patches and remedies, are shared as quickly as possible to avoid one attack cascading across the global financial system. The 2020 data breach, which was perpetrated through at least three technology companies that provide services to the financial sector, impacted the U.S. government, NATO, the U.K. government, and the European Parliament among others.[3] Although the targets here were not the financial sector, it is an important illustration of how far-reaching and widespread an attack can become if not quickly detected and mitigated.

The problem of market fragmentation

We greatly appreciate the FSB's efforts on this important issue and its recommendations towards a more harmonized global reporting framework. As the FSB has rightly identified in its previous consultation[4], and as has been detailed in a previous IIF Staff Paper,[5] CIR is often challenged by differing approaches and reporting requirements across various jurisdictions and authorities when it comes to what information is shared, in what format, and in what timeframe. There can be multiple policy objectives and different needs at play across the incident reporting landscape, such as providing early warning with actionable information and voluntary supplemental information sharing as an incident unfolds.

The IIF has in the past urged the FSB to encourage member jurisdictions to ensure that incident reporting requirements are simple, tied to an actionable purpose, and efficient. We also encouraged the FSB to highlight the importance of bidirectional sharing of reported information from authorities to FIs. Information related to material cyber incidents and widespread operational outages that is reported to authorities should be fed back to FIs, which can then take measures to bolster their cyber security and thereby enhance the resiliency of the sector.

If a cyber incident has occurred, firms would benefit from being able to launch processes and procedures in parallel instead of responding individually to jurisdictional stakeholders. Currently FIs are often faced with multiple jurisdictional and transnational reporting requirements, often with convoluted threshold-based analyses being required, which can increase time and effort spent on operational tasks and compliance at the time of an incident. These differences in reporting requirements are further compounded by differences and ambiguities in the terminology used, such as how firms and authorities define what constitutes a "cyber incident." Further, it is often the case that there is insufficient information sharing, including from financial authorities to FIs, and inadequate cross-border cooperation and collaboration. Together, these issues lead to fragmentation and divergence, unnecessarily slowing the ability of firms and authorities to respond to malicious threats.

[3] Wikipedia 2024. "2020 United States federal government data breach" Retrieved on November 25, 2024.
[4] FSB 2022. "Achieving Greater Convergence in Cyber Incident Reporting" October 17, 2022.
[5] IIF 2021. "IIF Paper on the Importance of More Effective Cyber Incident Reporting" June 10, 2021.

The value of the FIRE approach to cyber incident reporting

This iteration of FIRE (October 2024), which aims to promote common information elements for incident reporting while allowing for flexible implementation practices, has made a lot of progress in becoming a valuable public sector and industry standard. It is user friendly and bespoke, in that authorities can choose the extent to which they adopt FIRE, and leverage features and definitions to promote convergence and facilitate translation between existing frameworks. Of the 99 information items defined, 51 are optional, providing flexibility to authorities based on their own needs.

To make FIRE useful to a variety of authorities, whose own cyber incident reporting practices have grown organically, it is designed to cover operational incidents, including cyber incidents, extending the scope beyond the previous work on cyber resilience. There are common information items but importantly reporting triggers, deadlines and mitigation approaches are flexible. FIRE, as presently conceived, could also be leveraged by financial institutions in their relations with third-party service providers, thereby making it easier for institutions to report operational incidents that impact their ability to deliver agreed upon services or other obligations. At a later stage, if desirable, authorities can also apply FIRE to other parties, and other sectors, beyond financial services firms. At some point, if welcome, the FSB could also encourage other (non-financial) sectors to use the same template, to help address fragmentation across sectors.

A critical partnership between the public and private sectors

Another important characteristic of FIRE is that it is being closely developed with the private sector. The FSB has created an industry stakeholder advisory group, in which the IIF and several of its members participate. They have published consultations, organized workshops, and coordinated a discovery phase, design phase, and testing phase whereby financial institutions can test and experiment with FSB while it is being developed. The FSB has also committed to hosting an industry workshop in 2027, two years after the final version is released, to review experiences and to determine the needs for revisions.

This is a substantial achievement, and quite unusual for a global standard-setting body, who usually consult on issues where stakeholder feedback is welcome. It is perhaps a combination of the importance of addressing market fragmentation around cyber incident reporting, which can slow down mitigation at an important phase of a cyber incident; the fact that interests are closely aligned between the public and private sectors on mitigating cyber-attacks; but, also a strong willingness by the FSB and its members to find a solution that works for as many authorities and industry partners as possible.

The IIF has provided comments below to address different areas of discussion and recommendations in the consultation. We look forward to continued collaboration with the FSB throughout the stakeholder feedback process.

Broad Acceptance, and Distinction between Full and Partial Implementation

For FIRE to be most effective, it is important that as many authorities adopt it as their standard for having financial institutions report cyber incident reporting. The more authorities that can do this the better, and in doing so would substantially help address the current state of fragmentation around cyber incident reporting. Further harmonization can serve as a basis for aligning terms for data fields, data fields themselves and aligning on materiality triggers. On the other hand, the

fewer number of authorities that embrace FIRE, the more there is a risk that FIRE adds to the multiple approaches and fragmentation, a scenario that we all want to avoid. In that sense, the IIF and its members will work hard with the FSB to encourage the broad adoption of FIRE once it is finalized in mid-2025.

One tricky distinction is the option of partial implementation, which can offer coherence and interoperability benefits, but falls short of full implementation. Another one is the fact that of the 99 information items, only 48 are mandatory, and the majority (51) are optional. In both cases we would encourage authorities to strive for full implementation as their end goal, so that ultimately, even if partial implementation is the best that can be achieved at present, we progress towards much closer consistency globally. Furthermore, we encourage authorities try to avoid adopting data elements that are beyond the scope of FIRE because that would also contribute to more fragmentation and add additional fragmentation and inconsistency in an already complex environment.

Receiving Entities, recipient history, MOUs, and Onward Forwarding

An area that has sparked a lot of discussion is the sharing among authorities of information that they receive from the private sector. Authorities have long shared information on cyber threats and incidents with other authorities, in connection with their regulatory and supervisory activities, particularly as they pertain to financial services firms' cross-border operation. This cross-border sharing of information serves a number of important regulatory and supervisory purposes, but it can lead to the premature release of information beyond the scope of authorized parties. There are concerns that the ubiquity of FIRE, by facilitating information exchange among authorized parties, could increase the risk of unauthorized information flows. FI's would benefit from transparency as where the information is being forwarded to.

There are also considerations around the security of the information, given that the transmission of sensitive information to each additional recipient makes it increasingly likely that their sensitive information could be inadvertently mishandled. This is especially the case where the FSB requests firms to share sensitive information that could constitute a legal risk. The inclusion of 'legal and regulatory' information where the financial institution is expected to provide information concerning breaches. The FSB further asks for financial institutions to provide information on 'vulnerabilities exploited,' which is highly sensitive. IIF and its members encourage that both field types are removed and, in addition, strongly support the FSB's suggestions that forward and receiving recipients have comprehensive and stringently applied measures in place, including MoU clauses, technical controls, access controls, personnel vetting, and operating on a 'need to know' basis.

Another challenge is the fact that Company A might notify Country B and Country C when there is a cyber incident that impacts the business and operations in those jurisdictions, which would then be properly logged in the FIRE recipient history. If Country B and/or C sends this information to additional jurisdictions, these jurisdictions might take action against Company A for withholding information. The legal and regulatory risks could cause Company A to overreport at the outset in order to avoid liability, which could lead to challenges for authorities to identify truly important information when too much information is being reported.

Finally, there are questions around liability and the fact that incident reporting requires sharing information about other organizations. For example, if Company A reports in error that their software provider had a material breach, the third-party software provider could potentially take

legal action against Company A. One approach to this problem worth highlighting is the Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA), where institutions are granted liability protection when they submit reports about cyber incidents to the Cybersecurity and Infrastructure Security Agency (CISA), meaning that no legal action can be taken against them solely for reporting an incident, even if this protection does not shield them from liability for the underlying cyber incident itself.[6]

Importance of bidirectional information exchange

The IIF and its members have previously encouraged the FSB to support bidirectional sharing of reported information, including from authorities to FIs. To avoid cyber incidents spreading across the (global) financial system it is important that firms receive information related to material cyber incidents and operational outages that were reported to authorities. This way, the Fis can then take measures to bolster their cyber security and thereby enhance the resiliency of the sector.

There are of course organizations like FS-ISAC, which has been widely recognized as a global leader in threat intelligence sharing. The ISAC model has been successful in disseminating information in a timely and confidential manner to industry stakeholders on a voluntary basis. Incorporating established reporting practices can help strengthen the overall resilience of the financial system, especially for FIs and authorities at different stages of cyber security maturity. However, it remains the case that there is insufficient information-sharing from financial authorities to FIs, and inadequate cross-border cooperation and collaboration. Inadequate information sharing compounds the negative impacts of regulatory fragmentation and divergence, unnecessarily slowing the ability of firms and authorities to respond to malicious threats.

Materiality Thresholds

The IIF encourages the FSB to distinguish cyber incidents driven by malicious intent from non-malicious operational incidents given the criticality of prompt early warning to authorities and other potentially affected firms. Moreover, non-malicious operational incidents generally have different incident management policies, procedures, personnel, and reporting objectives when compared to malicious cyber incidents. Therefore, we think it worthwhile to limit reporting to incidents that cause actual harm and should rightly be prioritized so as to avoid a wider impact. We encourage the FSB to reiterate that its definitions for both operational and cyber incident are incidents that have an actual confirmed impacted (e.g., “has been determined to have an adverse impact” or “adversely affects.”)

We think it would be beneficial to include a materiality threshold, for non-malicious operational incidents occurring at both financial services firms and third-party service providers. FI’s should report material incidents only, as determined by each individual FI. To the extent that threshold can be made consistent across FSB member jurisdictions, the financial services sector would be able to respond and report more effectively.

Dividing affected parties into distinct groups, including vulnerable customers and consumers

When describing affected parties, authorities have the option of asking for the types of affected parties (see 1.3.2 on page 30), which includes several types of groups of possibly impacted

[6] CISA 2022. “Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA)” March 9, 2022.

parties. One of those categories is 'vulnerable customers/consumers' as a subset of 'customers/consumers.' While this may be important information for some authorities, especially if they have a consumer protection mandate, this information is generally not available at the beginning of the cyber incident reporting process, when information is still being discovered and resources are being dedicated to managing and mitigating the incident. Vulnerable customer impact is often more associated with services supporting retail banking services and is therefore a subset of the financial sector with minimal links to operational incidents or IT-impact. Requiring the provision of this information early in the reporting process could slow down both the incident management and the incident reporting processes. Accordingly, we would recommend that this option be removed, or at least deferred until the end of the cyber incident reporting cycle.

The value of FIRE for third-party reporting to financial institutions

In attempting to produce a framework that is useful across jurisdictions, and beneficial for both the public and private sector, there are strong arguments for wider applicability and adoption of FIRE for cyber incident reporting. As such, we support the suggestion that third parties should report material cyber incidents to other potentially affected financial institutions. In doing so, the information could be shared quickly and effectively by the FI with their authorities, which helps support a quicker response to these issues by both authorities and Fis.

In conclusion

We very much appreciate the opportunity to comment on this updated FSB version of FIRE. As noted above, the IIF and its members are strong supporters of information sharing and appreciate all the efforts being undertaken by the FSB and other authorities to protect and safeguard the global financial system. We believe FIRE will help address market fragmentation, and encourage the FSB to work collaboratively, and with other global standard-setters, to promote FIRE among constituent authorities to achieve a critical mass of early adopters.

We thank the FSB for its consideration of our comments and welcome any additional stakeholder engagement around this topic to help the FSB in its efforts to encourage and achieve greater convergence in cyber incident reporting. If you have any questions, please do not hesitate to contact Martin Boer at mboer@iif.com or Melanie Idler at midler@iif.com.

Sincerely,

Martin Boer
Senior Director, Regulatory Affairs
Institute of International Finance (IIF)