Format for Incident Reporting Exchange (FIRE): Consultation report

Response to Consultation

US Financial Services Sector Coordinating Council

General

1. **Please provide any general comments to the FIRE design. Please elaborate on the preconditions (for instance, extent of uptake by individual authorities, extent of convergence) you deem necessary in order for FIRE to be successful.**

   The Financial Service Sector Coordinating Council ('FSSCC') welcomes the opportunity to comment on the Financial Stability Board (FSB) Format for Incident Reporting Exchange (FIRE) Consultation Report." We value 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.

   This latest iteration of FIRE is focused on establishing common information elements for incident reporting while allowing flexibility in implementation. This effort has made significant strides toward becoming a recognized standard format for cyber incident reporting. Its user-friendly design allows authorities to determine the level of adoption that suits their needs, enabling them to utilize specific features and definitions to achieve harmonization and facilitate translation across existing frameworks. Out of the 99 defined information items, 51 are optional, granting authorities the flexibility to adapt based on their unique circumstances. While this flexibility is beneficial, it may on the other hand also lead to divergent regulatory practices across various jurisdictions.

   FIRE aims to be applicable to various authorities, also given that cyber incident reporting practices have developed organically across jurisdictions. It encompasses operational incidents, including cyber events, thereby broadening its focus beyond cyber resilience. While it includes common information items, it allows for flexible reporting triggers, deadlines, and mitigation strategies. Additionally, financial institutions can utilize FIRE in their interactions with third-party service providers, streamlining the reporting of operational incidents that impact service delivery or other obligations.

   Broad acceptance critical to eventual success

   To maximize FIRE's effectiveness, it is crucial for as many authorities as possible to adopt it as the standard format for financial institutions' cyber incident reporting. Increased adoption will help mitigate the current fragmentation in reporting practices. Conversely,

limited adoption could exacerbate existing discrepancies in regulatory approaches. Therefore, the FSSCC and its members recommend FSB members adopt FIRE once finalized in mid-2025.

Another consideration is partial implementation, which can provide coherence and interoperability but does not achieve the full benefits of complete implementation. Of the 99 information items, 51 are optional, which can lead to inconsistency even when jurisdictions have been implemented in full.

Authorities may also choose to extend FIRE's application to other sectors beyond financial services in the future. If beneficial, the FSB could promote the adoption of FIRE across non-financial sectors to help encourage cross-sectoral consistency.

The importance of public sector and industry collaboration

A key strength of the FIRE process has been the close collaboration with the private sector. The FSB has established an industry stakeholder advisory group, which includes the FSSCC and some of its members. This collaborative process has included consultations, workshops, and a phased approach allowing financial institutions to test FIRE's functionality as it develops. The FSB has also committed to hosting an industry workshop in 2027, two years post-release, to review experiences and identify revision needs.

This approach represents a significant achievement, as it is unusual for global standard-setting bodies to engage so deeply with stakeholders throughout the development process. This is based on both the urgency of reducing market fragmentation in cyber incident reporting—critical for efficient response when an incident arises—and the shared interests of public and private sectors in mitigating cyber threats.

Information sharing among authorities

The sharing of information among authorities based on private sector reporting is worth highlighting. Authorities have of course always exchanged threat and incident information. While this practice aids regulatory and supervisory activities, it risks unauthorized dissemination of sensitive information. The widespread adoption of FIRE may heighten this risk by facilitating information flows among authorized parties. Security concerns arise as sharing sensitive information increases the chances of inadvertent mishandling. We therefore support the FSB's recommendations for robust measures, including Memoranda of Understanding (MOUs), technical controls, access controls, personnel vetting, and operating on a strict "need to know" basis when authorities share incidents with each other.

Another challenge is the potential situation where Company A informs Country B and Country C about a cyber incident affecting operations in those jurisdictions. If Country B or C later shares this information with additional jurisdictions, those could take punitive action against Company A for perceived non-disclosure. This legal risk could lead to over-reporting by Company A to avoid liability.

There are also liability concerns associated with incident reporting that requires disclosing information about other organizations. For instance, if Company A incorrectly reports a major breach by their software provider, for example, and that turns out to be incorrect at a

later time, the provider might pursue legal action against them. The Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) offers a model for addressing this issue by protecting institutions from liability solely for reporting incidents, although it doesn't shield them from liability related to the incident itself.

Bidirectional information sharing

The FSSCC also encourages the FSB to promote bidirectional sharing of reported information between authorities and financial institutions. To prevent the spread of cyber incidents throughout the global financial system, it is crucial for firms to obtain information about significant cyber incidents and operational outages reported to authorities. This allows financial institutions to enhance their cybersecurity measures and improve the sector's resilience.

Organizations such as FS-ISAC are recognized leaders in threat intelligence sharing, successfully disseminating timely and confidential information to industry stakeholders on a voluntary basis. Integrating established reporting practices can fortify the overall resilience of the financial system, particularly for financial institutions and authorities operating at varying levels of cybersecurity maturity. However, there remains a significant gap in information sharing from financial authorities to financial institutions. This lack of information exchange exacerbates the challenges posed by regulatory fragmentation, hindering the ability of firms and authorities to respond effectively to malicious threats.

Materiality thresholds

The FSSCC encourages the FSB to differentiate between cyber incidents driven by malicious intent and non-malicious operational incidents, recognizing the importance of timely warnings for both authorities and potentially affected firms. Non-malicious operational incidents typically involve different management policies, procedures, personnel, and reporting objectives compared to malicious cyber incidents. Therefore, it is essential to focus reporting on incidents that result in actual harm, prioritizing them to minimize broader impacts.

We propose establishing a materiality threshold for non-malicious operational incidents affecting both financial services firms and third-party service providers. A consistent threshold across FSB member jurisdictions would enable reporting to be more efficient and actionable.

Identifying affected parties

When authorities identify affected parties, they can specify different categories, including 'vulnerable customers/consumers' as a subgroup of 'customers/consumers.' While this information is valuable for certain authorities, particularly those focused on consumer protection, it is often unavailable during the early stages of the cyber incident reporting process when details are still being uncovered, and resources are allocated to incident management. Mandating this information early in the reporting cycle could hinder both incident management and reporting efficiency. Therefore, we recommend that this option be removed or postponed until after the cyber incident reporting cycle is complete.

Value to Third-party parties of FIRE

To create a framework that effectively serves both public and private sectors across jurisdictions, we advocate for broader adoption of FIRE for cyber incident reporting. We support the idea that third parties should report significant cyber incidents to potentially affected financial institutions. This approach facilitates the quick and effective sharing of information from financial institutions to their authorities, fostering a faster response by both authorities and financial institutions.

Conclusion

The FSSCC appreciates the opportunity to provide comments on the Consultative Document and your consideration of the views expressed in this letter. The FSSCC welcomes further discussion and engagement on the topics raised in this letter. If you have any questions or need further information, please contact [REMOVED]

2. **Please give examples of the various ways in which FIRE can be used in your company's incident reporting, and/or of use cases of FIRE, and whether the design adequately facilitates these use cases.**

Scope of FIRE

3. **Is the FIRE design appropriately scoped? *(Choose: Not at all, Slightly, Moderately, Mostly, Completely).* Please elaborate. Which, if any, amendments to the definitions of 'operational', 'operational event', and 'operational incident' as used in FIRE, would be needed.**

4. **In addition to the primary scope covering incident reporting by financial institutions to their regulators, does the FIRE design appropriately facilitate its use for reporting of incidents to the financial institution by third-party service providers? *(Choose: Not at all, Slightly, Moderately, Mostly, Completely)*. Please elaborate. Which, if any, amendments to the current design would be helpful to fully cover this use case?**

Specific questions and technical questions

5. **For each of the FIRE pillars, is the design appropriate? Please consider: (a) number and nature of information elements, (b) their requested and permissible content, and (c) their relevance for the different reporting phases in the lifecycle of an incident.**

   (i) Reporting details (section 1.1 of the Design)

   (ii) Incident details (section 1.2 of the Design)

   (iii) Impact assessment (section 1.3 of the Design)

   (iv) Incident closure (section 1.4 of the Design)

For each FIRE pillar and each of subquestions (a) to (c), choose: Not at all, Slightly, Moderately, Mostly, Completely. Please provide comments in the related comment box for each FIRE pillar.

	(a)	(b)	(c)	Comment
(i)				
(ii)				
(iii)				
(iv)				

6. **Please provide any comments on the data model and/or the XBRL taxonomy that are part of the consultation package.**