# UK Finance response to the Financial Stability Board's Consultative Document "Achieving Greater Convergence in Cyber Incident Reporting"

**Date**: 29 December 2022

**Sent to**: fsb@fsb.org

UK Finance is the collective voice for the banking and finance industry. Representing more than 300 firms across the industry, we act to enhance competitiveness, support customers and facilitate innovation.

UK regulated FI Firms and FMIs already have significant regulatory and legislative commitments in the event of a of "cyber incident". Reporting obligations can pull resources away from responding to the event or incident, as such the mechanism for reporting needs to be as streamlined as possible.

Aspects of UK Finance membership hold strong views on the minimum benchmark of what would trigger the declaration of a "cyber incident". There is concern that; if placed too low, any objectively non-malicious outage could be categorised as a cyber incident and thus reportable under this framework.

The UK's financial sector maintains a robust framework for the sharing of actionable cyber threat intelligence both routinely and in the event of an incident.

Similar work is underway within the US financial sector, with the aim of bringing together currently disparate, state mandated, cyber incident reporting requirements under CISA's national authority and governance. Our members who have an international presence, request that the FSB's activities in this area coordinates with the work currently underway in the US. Furthermore, to avoid other international disparity, a review of all objectively significant "rest of world" financial sectors should be sought for similar projects (whether or not established or under development). Once the review has been completed, a top-down approach to cyber incident reporting should be adopted.

Any third party reporting requirements should be crafted to supplement reports from the third parties themselves, and be based on a meaningful degree of impact to the first party.

## Policy Objectives Should Drive Incident Information

Financial authorities' CIR requirements must align with clear and purposeful policy objectives. This is key because the policy objective determines what type of information a financial authority needs/asks for and what type of information a financial institution should provide. For example, if the financial authorities' intent is early warning, then financial institutions might only be required to notify the financial authority with high level incident information.

## Reporting Mechanisms.

In the event of any confirmed or possible cyber incident, UK regulated firms are already under a significant reporting burden. As such, due care needs to be given to any new reporting mechanism to ensure that firm's efforts can be focussed on addressing and resolving the situation rather than diverted to meeting their reporting obligations. As such, our membership supports the consultation

paper's recommendation 3 (adoption of common reporting formats) and recommendation 4 (implementation of phased and incremental reporting requirements).

In support of these recommendations, the FSB should encourage financial authorities to use a common, phased approach that differentiates between incident notification and incident reporting. Incident notification is the reporting mechanism for an "early warning" alert to financial authorities that a significant or materially impactful incident is occurring. This reporting mechanism enables financial institutions to quickly report high level information (frequently firms only have limited, high level information days after an incident) to financial authorities, while remaining focused on incident remediation. Once an incident is assessed and going through remediation, financial institutions could use incident reporting as the mechanism to report a more detailed analysis of the incident and its impact to financial authorities. This reporting mechanism enables financial institutions to focus on remediation in the immediate aftermath of an incident, while still providing incident information to financial authorities to help identify trends, common threats, or analysis of the effectiveness of security controls. Distinguishing between these two types of reporting will improve the ways in which financial authorities ask for and receive information that meets their regulatory objectives and will help financial institutions efficiently allocate their resources between compliance with reporting and remediation.

### The "cause agnostic" Definition of "cyber incident"

A number of UK Finance members have expressed their concerns to us that the consultation paper proposes that all incidents, whether malicious or not (referred to as "cause-agnostic" within the document), would be categorised as a cyber incident. Firms have expressed their concerns over the adoption of this approach due in-part to the perceived negative connotations of needing to frequently report or declare "incidents" when there are clear, early identifiable non-malicious causes and as such no sector level benefits from this information being shared.

> **UK Finance Comment:** The cited hypothetical situation given to UK Finance to help illustrate this point involves an inexperienced IT Admin making changes to the configuration of a system which is picked up by their internal Security Operations Centre as an incident. Within an hour the matter is resolved with no loss of data from the system and system redundancy meant that there was no discernible loss of service or additional systemic risk to the sector. The member stated that this can be a daily, if not weekly occurrence within a large multinational company with tens of thousands of network endpoints and their ability to detect, respond and recover from such events without needing to report externally is something that they value. Conversely, if the same exact incident occurred but the motivations of the IT Admin were nefarious, this would be an incident that they would report via the proposed regime.

### A Global Approach

UK Finance members with a global operational footprint have drawn our attention to similar efforts underway in the US. It is understood that the US's Cybersecurity & Infrastructure Security Agency (CISA), are looking to integrate States' individual requirements together. We would support the alignment of those goals with those of the FSB; and would go further to encourage a wider global approach.

> **UK Finance Comment:** Our members do not underestimate the scale of such a task being positively correlated with its difficulty. However, the added time and complexity of pan-global alignment on this issue is likely to pay dividends for the longevity of the relevance of the scheme it ultimately produces.

## Third Party Reporting Requirements

Any reporting requirements that form part of this regime should be crafted to supplement reports from the third parties themselves. To avoid the potential for the reported "cyber incident" to be viewed as two separate occurrences and mistakenly causing the misrepresentation of the volume of the incident, the reporting should be based on a meaningful degree of impact to the first party.

## Adoption of FIRE

Our membership concurs that, should FIRE be pursued it will be critical for the member's National Cyber Security Centres, National CERTS as well as FS-ISAC equivalents and MDR / SIEM Vendors be involved. It is recognised by the respondents to this consultation that FIRE reporting could be highly sensitive and become a potential target for threat actors, especially when aggregated, and the following recommended preconditions should be considered:

a. Defined secure communications method and process. For FIRE to succeed, trusted relationships need to exist between the public and private sectors. To promote trusted relationships, cyber incident information sharing needs to be secure and data must be protected and remain confidential (firm data should be anonymized if it shared from the financial authority to the financial industry). Financial institutions will be more likely to voluntarily share their incident information if financial authorities can guarantee data protection and security.
b. Automation enablement.
c. Defined recipients of FIRE reporting within each organisational entity (e.g., FI, Regulatory, National Cyber Security Centre).
d. Addressing identified sources of operational challenges.
e. Ensure that there is sufficient adoption levels and commitment within the FI community and wider G20 including a central design position across member countries.

## The Cyber Lexicon

Respondents have no specific concerns with the proposed amendments to the lexicon as set out in Table 1 of the document (page 23). Specifically, our membership agrees with the FSB's decision to remove "jeopardizes" from the definition of cyber incident because it limits the scope of incidents to those that cause actual or material harm. However, there is concern among some of our membership that certain definitions (specifically the definition of a cyber incident, aside from the aforementioned point regarding "cause agnosticism") are too wide reaching in scope. First, the current Cyber Lexicon puts any (whether minor or major) violation of security policies or procedures as a cyber incident. While the presence of these violations could lead to a cyber incident, they themselves are not always malicious cyber incidents. It is felt that if followed rigidly and may have the unintended outcome of creating a vast quantity of reported cyber incidents from which it will be difficult to discern which ones are of sector level importance. Second, there is a view that the FSB's definition of cyber incident should not cover non-malicious incidents as the term cyber incident necessarily means malicious intent. Specifically, the FSB should rephrase the last clause of the definition from "whether resulting from malicious activity or not" to read "resulting from malicious activity." Additionally, the following definitions should be revised as part of future lexicon reviews:

f. Compromise
g. Denial of Service

**UK Finance Comment:** It should be noted that the above viewpoint on defining the term "cyber incident", while important, does not represent all UK Finance respondents to the consultation paper. Some UK Finance members are both content with the current definitions as set out in the lexicon, and the suggested amendments even going further to state that the Cyber Lexicon

should be classed as a ‘mandatory requirement’ as part of a greater convergence in CIR. While we understand that this would have the benefit of ensuring that there is commonality across CIR reporting no matter where the report originated from, UK Finance recognises that this goes beyond the FSB’s remit.

### Reported Incidents Must Be Confirmed

As previously stated, we agree with the FSB’s decision to remove “jeopardizes” from the definition of cyber incident to limit the scope to incidents that cause “actual” harm. Firms and FIs need to be able to focus on confirmed, significant incidents as an influx of likely incidents could overwhelm financial authorities and drive financial institutions’ focus away from threat monitoring. Based on this argument, the FSB should not include “likely breaches” as it has done in Recommendation 8 (Extend materiality-based triggers to include likely breaches).

If you have any questions relating to this response, please contact Adam Avards, Principle Cyber & Third Party Risk at adam.avards@ukfinance.org.uk

**Adam Avards**
Principle, Cyber & Third Party Risk